(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 120 715 A1

(12) EUROPEAN PATENT APPLICATION

published in accordance with Art. 158(3) EPC

(43) Date of publication:
01.08.2001 Bulletin 2001/31

(21) Application number: **00944282.3**

(22) Date of filing: **06.07.2000**

(51) Int Cl.[7]: **G06F 15/00**, G06F 17/60, H04L 9/08, H04L 9/32, G10K 15/02, G06F 13/00

(86) International application number:
PCT/JP00/04488

(87) International publication number:
WO 01/02968 (11.01.2001 Gazette 2001/02)

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **06.07.1999 JP 19241399**
07.07.1999 JP 19356199
07.07.1999 JP 19356299
21.04.2000 JP 2000126305

(71) Applicant: **Sony Corporation**
Tokyo 141-0001 (JP)

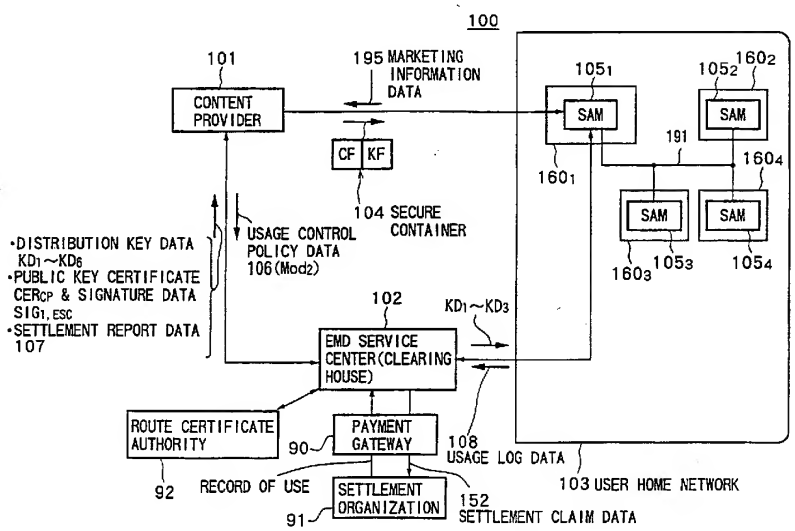
(72) Inventors:
- **NONAKA, Akira Sony Corporation**
Tokyo 141-0001 (JP)
- **EZAKI, Tadashi Sony Corporation**
Tokyo 141-0001 (JP)

(74) Representative: **Melzer, Wolfgang, Dipl.-Ing. et al**
Patentanwälte
Mitscherlich & Partner,
Sonnenstrasse 33
80331 München (DE)

(54) DATA PROVIDING SYSTEM, DEVICE, AND METHOD

(57) A content provider 101 distributes a secure container 104 storing content data encrypted using content key data, content key data encrypted using distribution key data, and encrypted usage control policy data indicating the handling of the content data to a SAM 105_1 of a user home network 103 etc. The SAM 105_1 etc. decrypts the content data and usage control policy data stored in the secure container 104 and determines the purchase mode and usage mode and other handling of the content data based on said decrypted usage control policy data.

FIG.1



EP 1 120 715 A1

Description

TECHNICAL FIELD

[0001] The present invention relates to a data providing system and a data providing apparatus and methods of the same for providing content data and a management apparatus and a data processing apparatus used in the same.

BACKGROUND ART

[0002] There is a data providing system for distributing encrypted content data to data processing apparatuses of users concluding a predetermined contract and comprising the related data processing apparatuses decrypt, reproduce, and store the content data.

[0003] As one of such data providing systems, there is a conventional EMD (electronic music distribution) system for distributing music data.

[0004] Figure 100 is a view of the configuration of a conventional EMD system 700.

[0005] In the EMD system 700 shown in Fig. 100, content providers 701a and 701b encrypt content data 704a, 704b, and 704c and copyright information 705a, 705b, and 705c by session key data obtained after mutual authentication and supply them to a service provider 710 on-line or off-line. Here, the copyright information 705a, 705b, and 705c include for example SCMS (serial copy Management system) information, electronic watermark information requesting burying in content data, and information concerning the copyright requesting burying in a transmission protocol of the service provider 710.

[0006] The service provider 710 decrypts the received content data 704a, 704b, and 704c and copyright information 705a, 705b, and 705c by using the session key data.

[0007] Then, the service provider 710 buries the copyright information 705a, 705b, and 705c in the content data 704a, 704b, and 704c decrypted or received off-line to generate content data 707a, 707b, and 707c. At this time, the service provider 710 changes a predetermined frequency domain of for example the electronic watermark information in the copyright information 705a, 705b, and 705c and buries it in the content data 704a, 704b, and 704c and buries the SCMS information in a network protocol used when transmitting the related content data to the user.

[0008] Further, the service provider 710 encrypts the content data 707a, 707b, and 707c by using content key data Kca, Kcb, and Kcc read from a key database 706. Thereafter, the service provider 710 encrypts a secure container 722 with the encrypted content data 707a, 707b, and 707c stored therein by the session key data obtained after the mutual authentication and transmits the same to a CA (conditional access) module 711 existing in terminal equipment 709 of the user.

[0009] The CA module 711 decrypts the secure container 722 by using the session key data. Further, the CA module 711 receives the content key data Kca, Kcb, and Kcc from the key database 706 of the service provider 710 by using an electronic settlement and CA or other charging function and decrypts them by using the session key data. Due to this, in the terminal equipment 709, it becomes possible to decrypt the content data 707a, 707b, and 707c by using the content key data Kca, Kcb, and Kcc.

[0010] At this time, the CA module 711 performs charge processing in units of content, generates charging information 721 in accordance with the result of this, encrypts this by the session key data, and then transmits the same to a right clearing module 720 of the service provider 710.

[0011] In this case, the CA module 711 collects the items it desires to manage relating to the service provided by the service provider 710 itself, that is, the contract (update) information of the user and the monthly base fee or other network rent, performs charge processing in units of content, and secures the security of a physical layer of the network.

[0012] The service provider 710 distributes profit between the service provider 710 and the content providers 701a, 701b, and 701c when receiving the charge information 721 from the CA module 711.

[0013] At this time, the profit is distributed from the service provider 710 to the content providers 701a, 701b, and 701c via for example the JASRAC (Japanese Society for Rights of Authors, Composers, and Publishers). Further, the profit of the content provider is distributed to the copyright owner, artist, song writer and/or composer, and affiliated production company of the related content data by the JASRAC.

[0014] Further, the terminal equipment 709, when storing the content data 707a, 707b, and 707c decrypted by using the content key data Kca, Kcb, and Kcc in a RAM type storage medium 723 or the like, rewrites the SCMS bits of the copyright information 705a, 705b, and 705c to control copying. Namely, the user side controls copying to protect the copyright based on the SCMS bits buried in the content data 707a, 707b, and 707c.

[0015] The SCMS was established for preventing storing from a CD (compact disc) to a DAT (digital audio tape). Copying between one DAT and another DAT is still possible. Further, even when burying electronic watermark information in the content data, when a problem arises, only the content provider which provided the content data concerned is specified. Illegal copying is not prevented by technical means.

[0016] Accordingly, in the EMD system 700 shown in Fig. 100, there is the problem in that the right (profit) of the content provider is not sufficiently protected.

[0017] Further, in the above EMD system 700, since the copyright information of the content provider is buried in the content data by the service provider, the content provider must inspect if the information has been

buried as requested. Further, the content provider must inspect if the service provider has distributed the content data as contracted. For this reason, there is the problem that the load for the inspection is large.

[0018] Further, in the EMD system 700, the charging information 721 from the terminal equipment 709 of the user is processed by the right clearing module 720 of the service provider 710, so there is a concern if the profit which should be received by the content provider in accordance with the usage of the content data by the user can be suitably received by the content provider.

DISCLOSURE OF THE INVENTION

[0019] The present invention was made in consideration with the problem of the above related art and has as an object thereof to provide a data providing system and a data providing apparatus and methods of the same and a data processing apparatus and a management apparatus capable of suitably protecting the profits of the owners of rights (related parties) of a content provider.

[0020] Further, the present invention has as another object the provision of a data providing system and a data providing apparatus and methods of the same and a data processing apparatus and a management apparatus capable of reducing the load of the inspection for protecting the profits of the owners of rights of a content provider.

[0021] In order to solve the problems of the prior art and achieve the above objects, the data providing system of a first aspect of the present invention is a data providing system for distributing content data from a data providing apparatus to a data processing apparatus, wherein the data providing apparatus distributes a module storing the content data encrypted by using content key data, encrypted content key data, and an encrypted usage control policy data indicating handling of the content data to the data processing apparatus and wherein the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed module and determines the handling of the content data based on the related decrypted usage control policy data.

[0022] In the data providing system of the first aspect of the invention, the module storing the content data encrypted by using the content key data, the encrypted content key data, and the encrypted usage control policy data indicating the handling of the content data is distributed from the data providing apparatus to the data processing apparatus.

[0023] Then, in the data processing apparatus, the content key data and the usage control policy data stored in the distributed module are decrypted, and the handling of the content data is determined based on the related decrypted usage control policy data.

[0024] By storing the usage control policy data indicating the handling of the related content data in the module storing the content data in this way, in the data processing apparatus, it becomes possible to handle (use) the content data based on the usage control policy data generated by related parties of the data providing apparatus.

[0025] Further, in the data providing system of the first aspect of the invention, preferably the data providing apparatus distributes the module storing the encrypted content key data and the usage control policy data to the data processing apparatus by using distribution key data, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed module by using the distribution key data.

[0026] Further, the data providing system of the first aspect of the invention preferably further has a management apparatus for managing the distribution key data and distributing the distribution key data to the data providing apparatus and the data processing apparatus.

[0027] Further, a data processing apparatus of a second aspect of the invention is a data processing apparatus utilizing content data distributed from a data providing apparatus, which receives a module storing content data encrypted by using content key data, encrypted content key data, and encrypted usage control policy data indicating the handling of the content data from the data providing apparatus, decrypts the content key data and the usage control policy data stored in the related received module, and determines the handling of the content data based on the related decrypted usage control policy data.

[0028] Further, a data providing system of a third aspect of the invention is a data providing system comprising a data providing apparatus, a data distribution apparatus, and a data processing apparatus, wherein the data providing apparatus provides a first module storing content data encrypted by using content key data, encrypted content key data, and encrypted usage control policy data indicating the handling of the content data to the data distribution apparatus, the data distribution apparatus distributes a second module storing the encrypted content data, content key data, and usage control policy data stored in the provided first module to the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed second module and determines the handling of the content data based on the related decrypted usage control policy data.

[0029] In the data providing system of the third aspect of the invention, the first module storing the content data encrypted by using the content key data, encrypted content key data, and encrypted usage control policy data indicating the handling of the content data is provided from the data providing apparatus to the data distribution apparatus.

[0030] Next, the second module storing the encrypted content data, content key data, and usage control policy data stored in the provided first module is distributed

from the data distribution apparatus to the data processing apparatus.

[0031] Next, in the data processing apparatus, the content key data and the usage control policy data stored in the distributed second module are decrypted, and the handling of the content data is determined based on the related decrypted usage control policy data.

[0032] Further, in the data providing system of the third aspect of the invention, preferably the data distribution apparatus distributes the second module storing price data indicating the price of the content data to the data processing apparatus.

[0033] Further, a data providing system of a fourth aspect of the invention is a data providing system comprising a data providing apparatus, at least a first data distribution apparatus and a second data distribution apparatus, and a data processing apparatus, wherein the data providing apparatus provides a first module storing content data encrypted by using content key data, encrypted content key data, and encrypted usage control policy data indicating the handling of the content data to the plurality of data distribution apparatuses, the first data distribution apparatus distributes the second module storing the encrypted content data, content key data, and usage control policy data stored in the provided first module to the data processing apparatus, the second data distribution apparatus distributes a third module storing the encrypted content data, content key data, and usage control policy data stored in the provided first module to the data processing apparatus, and the data processing apparatus decrypts the content key data and the usage control policy data stored in the distributed second module and the third module and determines the handling of the content data based on the related decrypted usage control policy data.

[0034] Further, a data providing system of a fifth aspect of the invention is a data providing system comprising at least a first data providing apparatus and a second data providing apparatus, a data distribution apparatus, and a data processing apparatus, wherein the first data providing apparatus provides a first module storing first content data encrypted by using first content key data, encrypted first content key data, and encrypted first usage control policy data indicating the handling of the first content data to the data distribution apparatus, the second data providing apparatus provides a second module storing second content data encrypted by using second content key data, encrypted second content key data, and encrypted second usage control policy data indicating the handling of the second content data to the data distribution apparatus, the data distribution apparatus distributes a third module storing the encrypted first content data, the first content key data, and the first usage control policy data stored in the provided first module and the encrypted second content data, the second content key data, and the second usage control policy data stored in the provided second module to the data processing apparatus, and the data processing apparatus decrypts the first content key data and the first usage control policy data stored in the distributed third module, determines the handling of the first content data based on the related decrypted first usage control policy data, decrypts the second content key data and the second usage control policy data stored in the distributed third module, and determines the handling of the second content data based on the related decrypted second usage control policy data.

[0035] Further, a data providing apparatus of a sixth aspect of the invention is a data providing apparatus for distributing content data to a data processing apparatus for using the content data and distributes a module storing content data encrypted by using the content key data, encrypted content key data, and encrypted usage control policy data indicating the handling of the content data to the data processing apparatus.

[0036] Further, a data providing method of a seventh aspect of the invention is a data providing method for distributing content data from a data providing apparatus to a data processing apparatus, comprising the steps of distributing a module storing content data encrypted by using content key data, encrypted content key data, and encrypted usage control policy data indicating the handling of the content data from the data providing apparatus to the data processing apparatus and having the data processing apparatus decrypt the content key data and the usage control policy data stored in the distributed module and determine the handling of the content data based on the related decrypted usage control policy data.

[0037] Further, a data providing method of an eighth aspect of the invention is a data providing method using a data providing apparatus, data distribution apparatus, and data processing apparatus, comprising the steps of providing a first module storing content data encrypted by using content key data, encrypted content key data, and encrypted usage control policy data indicating the handling of the content data from the data providing apparatus to the data distribution apparatus, distributing a second module storing the encrypted content data, content key data, and usage control policy data stored in the provided first module from the data distribution apparatus to the data processing apparatus, and having the data processing apparatus decrypt the content key data and the usage control policy data stored in the distributed second module and determine the handling of the content data based on the related decrypted usage control policy data.

[0038] Further, a data providing method of a ninth aspect of the invention is a data providing method using a data providing apparatus, at least a first data distribution apparatus and second data distribution apparatus, and a data processing apparatus, comprising the steps of providing a first module storing content data encrypted by using content key data, encrypted content key data, and encrypted usage control policy data indicating the

handling of the content data from the data providing apparatus to the data distribution apparatuses, distributing a second module storing the encrypted content data, content key data, and usage control policy data stored in the provided first module from the first data distribution apparatus to the data processing apparatus, distributing a third module storing the encrypted content data, content key data, and usage control policy data stored in the provided first module from the second data distribution apparatus to the data processing apparatus, and having the data processing apparatus decrypt the content key data and the usage control policy data stored in the distributed second module and the third module and determine the handling of the content data based on the related decrypted usage control policy data.

[0039] Further, a data providing method of a 10th aspect of the invention is a data providing method using at least a first data providing apparatus and second data providing apparatus, a data distribution apparatus, and a data processing apparatus, comprising the steps of providing a first module storing first content data encrypted by using first content key data, encrypted first content key data, and encrypted first usage control policy data indicating the handling of the first content data from the first data providing apparatus to the data distribution apparatus, providing a second module storing second content data encrypted by using second content key data, encrypted second content key data, and encrypted second usage control policy data indicating the handling of the second content data from the second data providing apparatus to the data distribution apparatus, distributing a third module storing the encrypted first content data, the first content key data, and the first usage control policy data stored in the provided first module and the encrypted second content data, the second content key data, and the second usage control policy data stored in the provided second module from the data distribution apparatus to the data processing apparatus, and having the data processing apparatus decrypt the first content key data and the first usage control policy data stored in the distributed third module, determine the handling of the first content data based on the related decrypted first usage control policy data, decrypt the second content key data and the second usage control policy data stored in the distributed third module, and determine the handling of the second content data based on the related decrypted second usage control policy data

[0040] Further, a data providing system of an 11th aspect of the invention is a data providing system comprising a data providing apparatus, data processing apparatus, and management apparatus, wherein the data providing apparatus distributes content data and usage control policy data indicating the handling of the related content data to the data processing apparatus and requests to the management apparatus to certify legitimacy of the usage control policy data, the data processing apparatus uses the distributed content data based on the distributed usage control policy data, and the management apparatus manages the data providing apparatus and the data processing apparatus and certifies the legitimacy of the usage control policy data in response to a request from the data providing apparatus.

[0041] At this time, the legitimacy of the usage control policy data is certified by the management apparatus by the management apparatus preparing for example signature data with respect to the usage control policy data.

[0042] In the data providing system of the 11th aspect of the invention, the content data and the usage control policy data indicating the handling of the related content data are distributed from the data providing apparatus to the data processing apparatus.

[0043] Next, the data processing apparatus uses the distributed content data based on the distributed usage control policy data.

[0044] Further, the legitimacy of the usage control policy data is certified in the management apparatus in response to a request from the data providing apparatus.

[0045] Further, in the data providing system of the 11th aspect of the invention, preferably the data providing apparatus makes the request by transmitting a module storing the usage control policy data, its own identifier, and at least signature data generated by using its own secret key data with respect to the usage control policy data to the management apparatus.

[0046] Further, in the data providing system of the 11th aspect of the invention, preferably the management apparatus distributes public key certificate data for certifying the legitimacy of the public key data corresponding to the secret key data of the data providing apparatus to the data providing apparatus together with the signature data generated by using its own secret key data, and the data providing apparatus makes a request by transmitting a module storing the public key certificate data, the usage control policy data, its own identifier, and the signature data to the management apparatus.

[0047] Further, in the data providing system of the 11th aspect of the invention, preferably the management apparatus manages distribution key data, distributes the related distribution key data to the data processing apparatus, generates signature data generated by using its own secret key data with respect to the usage control policy data in response to a request from the data providing apparatus, encrypts a module storing the related generated signature data and the usage control policy data by using the distribution key data, and transmits the same to the data providing apparatus, the data providing apparatus distributes a module received from the management apparatus to the data processing apparatus, and the data processing apparatus decrypts the module received from the data providing apparatus by using the distribution key data, verifies the legitimacy of the signature data stored in the related module by using the public key data of the management apparatus, and uses the distributed content data based on the us-

age control policy data stored in the module when it decides it is legitimate.

[0048] Further, a data providing system of a 12th aspect of the invention is a data providing system comprising a data providing apparatus, data processing apparatus, and management apparatus, wherein the data providing apparatus encrypts content data by using content key data, distributes the related encrypted content data to the data processing apparatus, and requests to the management apparatus to certify the legitimacy of the content key data, the data processing apparatus decrypts the distributed content data by using the content key data and uses the related decrypted content data, and the management apparatus manages the data providing apparatus and the data processing apparatus and certifies the legitimacy of the content key data in response to a request from the data providing apparatus.

[0049] In the data providing system of the 12th aspect of the invention, the content data encrypted by using the content key data is distributed from the data providing apparatus to the data processing apparatus.

[0050] Next, the data processing apparatus decrypts the distributed content data by using the content key data and uses the related decrypted content data.

[0051] Further, the legitimacy of the content key data is certified in the management apparatus in response to a request from the data providing apparatus.

[0052] Further, a data providing system of a 13th aspect of the invention is a data providing system comprising a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus, wherein the data providing apparatus provides content data and usage control policy data indicating the handling of the related content data to the data distribution apparatus and requests to the management apparatus to certify the legitimacy of the usage control policy data, the data distribution apparatus distributes the provided content data and the usage control policy data to the data processing apparatus, the data processing apparatus uses the distributed content data based on the distributed usage control policy data, and the management apparatus manages the data providing apparatus and the data processing apparatus and certifies the legitimacy of the usage control policy data in response to a request from the data providing apparatus.

[0053] In the data providing system of the 13th aspect of the invention, the content data encrypted by using the content key data is distributed from the data providing apparatus to the data processing apparatus.

[0054] Next, the data processing apparatus decrypts the distributed content data by using the content key data and uses the related decrypted content data.

[0055] Further, the legitimacy of the content key data is certified in the management apparatus in response to a request from the data providing apparatus.

[0056] A data providing system of a 14th aspect of the invention is a data providing system comprising a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus, wherein the data providing apparatus encrypts content data by using content key data, provides related encrypted content data, and usage control policy data indicating the handling of the related content data to the data distribution apparatus, and requests to the management apparatus to certify the legitimacy of the content key data, the data distribution apparatus distributes the provided content data and the usage control policy data to the data processing apparatus, the data processing apparatus uses the content data containing the decryption of the content data using the content key data based on the distributed usage control policy data, and the management apparatus manages the data providing apparatus and the data processing apparatus and certifies the legitimacy of the content key data in response to a request from the data providing apparatus.

[0057] In the data providing system of the 14th aspect of the invention, the content data encrypted by using the content key data and usage control policy data indicating the handling of the related content data are provided from the data providing apparatus to the data distribution apparatus.

[0058] Next, the content data and the usage control policy data provided from the data distribution apparatus to the data processing apparatus are distributed to the data processing apparatus.

[0059] Next, the data processing apparatus uses the content data containing the decryption of the content data using the content key data based on the distributed usage control policy data.

[0060] Further, the management apparatus certifies the legitimacy of the content key data in response to a request from the data providing apparatus.

[0061] Further, a management apparatus of a 15th aspect of the invention is a management apparatus for managing a data providing apparatus for distributing content data and usage control policy data indicating the handling of the related content data and a data processing apparatus for using the distributed content data based on the distributed usage control policy data and certifies the legitimacy of the usage control policy data in response to a request from the data providing apparatus.

[0062] Further, a management apparatus of a 16th aspect of the invention is a management apparatus for managing a data providing apparatus for distributing content data encrypted by using content key data and usage control policy data indicating the handling of the related content data and a data processing apparatus for decrypting the content data distributed based on the distributed usage control policy data by using the content key data, then using the related content data and certifies the legitimacy of the content key data in response to a request from the data providing apparatus.

[0063] Further, a management apparatus of a 17th

aspect of the invention is a management apparatus for managing a data providing apparatus for providing content data and usage control policy data indicating the handling of the related content data, a data distribution apparatus for distributing the provided content data and the usage control policy data, and a data processing apparatus for using the content data distributed based on the distributed usage control policy data and certifies the legitimacy of the usage control policy data in response to a request from the data providing apparatus.

[0064] Further, a data providing method of an 18th aspect of the invention is a data providing method using a data providing apparatus, data processing apparatus, and management apparatus, comprising the steps of distributing content data and usage control policy data indicating the handling of the related content data from the data providing apparatus to the data processing apparatus, having the data processing apparatus use the distributed content data based on the distributed usage control policy data, and certifying the legitimacy of the usage control policy data in the management apparatus in response to a request from the data providing apparatus.

[0065] Further, a data providing method of a 19th aspect of the invention is a data providing method using a data providing apparatus, data processing apparatus, and management apparatus, comprising the steps of distributing content data encrypted by using content key data from the data providing apparatus to the data processing apparatus, having the data processing apparatus decrypt the distributed content data by using the content key data, and certifying the legitimacy of the content key data in the management apparatus in response to a request from the data providing apparatus.

[0066] Further, a data providing method of a 20th aspect of the invention is a data providing method using a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus, comprising the steps of providing content data and usage control policy data indicating the handling of the related content data from the data providing apparatus to the data distribution apparatus, distributing the provided content data and the usage control policy data from the data distribution apparatus to the data processing apparatus, having the data processing apparatus use the distributed content data based on the distributed usage control policy data, and certifying the legitimacy of the usage control policy data in the management apparatus in response to a request from the data providing apparatus.

[0067] Further, a data providing method of a 21st aspect of the invention is a data providing method using a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus, comprising the steps of providing content data encrypted by using content key data and usage control policy data indicating the handling of the related content data from the data providing apparatus to the data distribution apparatus, distributing the content data and the usage control policy data provided from the data distribution apparatus to the data processing apparatus to the data processing apparatus, using the content data containing the decryption of the content data using the content key data based on the distributed usage control policy data in the data processing apparatus, and certifying the legitimacy of the content key data in the management apparatus in response to a request from the data providing apparatus.

[0068] Further, a data providing system of a 22nd aspect of the invention is a data providing system comprising a data providing apparatus, data processing apparatus, and management apparatus, wherein the data providing apparatus distributes content data and usage control policy data indicating the handling of the related content data to the data processing apparatus, the data processing apparatus determines at least one of a purchase mode and a usage mode of the distributed content data based on the distributed usage control policy data and transmits log data indicating the log of at least one of the related determined purchase mode and usage mode to the management apparatus, and the management apparatus manages the data providing apparatus and the data processing apparatus and performs profit distribution processing for distributing the profit obtained accompanied with the purchase and the usage of the content data in the data processing apparatus to related parties of the data providing apparatus based on received log data.

[0069] In the data providing system of the 22nd aspect of the invention, the content data and the usage control policy data indicating the handling of the related content data are distributed from the data providing apparatus to the data processing apparatus.

[0070] Next, the data processing apparatus determines at least one of the purchase mode and the usage mode of the distributed content data based on the distributed usage control policy data.

[0071] Next, the log data indicating the log of at least one of the related determined purchase mode and usage mode is transmitted from the data processing apparatus to the management apparatus.

[0072] Next, the management apparatus manages the data providing apparatus and the data processing apparatus and perform the profit distribution processing for distributing the profit obtained accompanied with the purchase and the usage of the content data in the data processing apparatus to related parties of the data providing apparatus based on the received log data.

[0073] Further, a data providing system of a 23rd aspect of the invention is a data providing system comprising a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus, wherein the data providing apparatus provides content data and usage control policy data indicating the handling of the related content data to the data distribution apparatus, the data distribution apparatus distrib-

utes the provided content data and the usage control policy data to the data processing apparatus, the data processing apparatus has a first module for communicating with the data distribution apparatus and a second module for determining at least one of a purchase mode and usage mode of the distributed content data based on the distributed usage control policy data and transmitting log data indicating the log of the related determined purchase mode and usage mode to the management apparatus, and the management apparatus manages the data providing apparatus, data distribution apparatus, and data processing apparatus and performs profit distribution processing for distributing the profit obtained accompanied with the data processing apparatus receiving the distribution of the content data and purchasing and using the content data to related parties of the data providing apparatus and the data distribution apparatus based on the log data received from the second module.

[0074] In the data providing system of the 23rd aspect of the invention, the content data and the usage control policy data indicating the handling of the related content data are provided from the data providing apparatus to the data distribution apparatus.

[0075] Next, the provided content data and the usage control policy data are distributed from the data distribution apparatus to the data processing apparatus.

[0076] Next, the data processing apparatus determines at least one of the purchase mode and the usage mode of the distributed content data based on the distributed usage control policy data.

[0077] Next, the log data indicating the log of the determined purchase mode and usage mode is transmitted from the data processing apparatus to the management apparatus.

[0078] Next, the management apparatus performs profit distribution processing for distributing the profit obtained accompanied with the data processing apparatus receiving the distribution of the content data and purchasing and using the content data to related parties of the data providing apparatus and the data distribution apparatus based on the received log data.

[0079] Further, a data providing system of a 24th aspect of the invention is a data providing system comprising a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus, wherein the data providing apparatus provides content data and usage control policy data indicating the handling of the related content data to the data distribution apparatus, the data distribution apparatus distributes the provided content data and the usage control policy data to the data processing apparatus and performs charge processing concerning the distribution of the content data based on a data distribution apparatus use purchase log data received from the data processing apparatus, the data processing apparatus has a first module for creating the data distribution apparatus use purchase log data indicating the log of the purchase of the content data distributed from the data distribution apparatus and transmitting the same to the data distribution apparatus and a second module for determining at least one of the purchase mode and the usage mode of the distributed content data based on the distributed usage control policy data and transmitting a management apparatus use log data indicating the log of the related determined purchase mode and usage mode to the management apparatus, and the management apparatus performs profit distribution processing for distributing the profit obtained accompanied with the purchase and the usage of the content data in the data processing apparatus to related parties of the data providing apparatus and the data distribution apparatus based on the management apparatus use log data.

[0080] Further, a data providing system of a 25th aspect of the invention is a data providing system comprising a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus, wherein the data providing apparatus provides the content data to the data distribution apparatus, the data distribution apparatus distributes the provided content data to the data processing apparatus, the data processing apparatus uses the distributed content data, and the management apparatus manages operation of a data providing service by the data providing apparatus, the data distribution apparatus, and the data processing apparatus.

[0081] Further, a data providing system of a 26th aspect of the invention is a data providing system comprising a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus, wherein the data providing apparatus provides content data to the data distribution apparatus, the data distribution apparatus distributes the provided content data to the data processing apparatus, the data processing apparatus uses the distributed content data, and the management apparatus manages the operation of a data providing service by the data providing apparatus, the data distribution apparatus, and the data processing apparatus, wherein the transmission of data among the data providing apparatus, the data distribution apparatus, the data processing apparatus, and the management apparatus is carried out by using mutual authentication using a public key encryption method, signature creation, signature verification, and encryption of data by a common key encryption method.

[0082] Further, a data providing system of a 27th aspect of the invention is a data providing system comprising a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus, wherein the data providing apparatus provides content data to the data distribution apparatus, the data distribution apparatus distributes the provided content data to the data processing apparatus, the data processing apparatus uses the distributed content data, and the management apparatus manages the operation of a data providing service by the data providing appa-

ratus, the data distribution apparatus, and the data processing apparatus, generates signature data indicating that the related data is generated by itself by using its own secret key data when each of the data providing apparatus, the data distribution apparatus, and the data processing apparatus supplies the data to another apparatus, and generates and manages public key certificate data of public key data corresponding to the secret key data of the data providing apparatus, the data distribution apparatus, and the data processing apparatus when the legitimacy of the signature data corresponding to the data is verified by using the public key data of the related other apparatus when receiving the supply of the related data from the other apparatus, wherein the data providing apparatus, the data distribution apparatus, and the data processing apparatus acquire the their own public key certificate data from the management apparatus before communicating with the other apparatus and transmit the related acquired public key certificate data to the other apparatus.

[0083] Further, a data providing system of a 28th aspect of the invention is a data providing system comprising a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus, the data providing apparatus provides content data to the data distribution apparatus, the data distribution apparatus distributes the provided content data to the data processing apparatus, the data processing apparatus uses the distributed content data, and the management apparatus manages the operation of a data providing service by the data providing apparatus, the data distribution apparatus, and the data processing apparatus, generates the signature data indicating that the related data is generated by itself by using its own secret key data when each of the data providing apparatus, the data distribution apparatus, and the data processing apparatus supplies data to another apparatus, and generates and manages public key certificate data of public key data corresponding to the secret key data of the data providing apparatus, the data distribution apparatus, and the data processing apparatus when the legitimacy of the signature data corresponding to the data is verified by using the public key data of the related other apparatus when receiving the supply of the related data from the other apparatus, wherein the data providing apparatus, the data distribution apparatus, and the data processing apparatus acquire their own public key certificate data from the management apparatus before communicating with the other apparatus and transmit the related acquired public key certificate data to the other apparatus at the communication.

[0084] Further, a data providing system of a 29th aspect of the invention has a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus, wherein the data providing apparatus provides content data to the data distribution apparatus, the data distribution apparatus distributes the provided content data to the data processing apparatus, the data processing apparatus uses the distributed content data, and the management apparatus manages the operation of a data providing service by the data providing apparatus, the data distribution apparatus, and the data processing apparatus, generates signature data indicating that the related data is generated by itself by using its own secret key data when each of the data providing apparatus, the data distribution apparatus, and the data processing apparatus supplies data to another apparatus, generates and manages public key certificate data of public key data corresponding to the secret key data of the data providing apparatus, the data distribution apparatus, and the data processing apparatus when the legitimacy of the signature data corresponding to the data is verified by using the public key data of the related other apparatus when receiving the supply of the related data from the other apparatus, and generates a public key certificate revocation list for specifying public key certificate data to be invalidated among the generated public key certificate data and thereby to restrict the communication or the distribution using public key certificate data specified by the public key certificate revocation list by the data providing apparatus, the data distribution apparatus, and the data processing apparatus.

[0085] Further, a data providing system of a 30th aspect of the invention has a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus, wherein the data providing apparatus provides content data to the data distribution apparatus, the data distribution apparatus distributes the provided content data to the data processing apparatus, the management apparatus manages the operation of a data providing service by the data providing apparatus, the data distribution apparatus, and the data processing apparatus, generates signature data indicating that the related data is generated by an apparatus itself by using its own secret key data when the data providing apparatus supplies data to another apparatus, generates and manages public key certificate data of public key data corresponding to the secret key data of the data providing apparatus for when another apparatus verifies the legitimacy of the related signature data by using the public key data corresponding to the secret key data, generates a public key certificate revocation list for specifying public key certificate data to be invalidated among the generated public key certificate data, distributes the related public key certificate revocation list to the data processing apparatus, and the data processing apparatus verifies whether or not public key certificate data of the data providing apparatus providing the distributed content data is invalid based on the public key certificate revocation list distributed from the management apparatus and controls the usage of the distributed content data based on the result of the related verification.

[0086] Further, a data providing system of a 31st aspect of the invention has a data providing apparatus, da-

ta distribution apparatus, data processing apparatus, and management apparatus, wherein the management apparatus manages the operation of a data providing service by the data providing apparatus, the data distribution apparatus, and the data processing apparatus, generates signature data indicating that the related data is generated by an apparatus itself by using its own secret key data when the data providing apparatus supplies data to another apparatus, generates and manages public key certificate data of public key data corresponding to the secret key data of the data providing apparatus for when another apparatus verifies the legitimacy of the related signature data by using the public key data corresponding to the secret key data, generates a public key certificate revocation list for specifying public key certificate data to be invalidated among the generated public key certificate data, distributes the related public key certificate revocation list to the data distribution apparatus, and the data distribution apparatus verifies whether or not public key certificate data of the data providing apparatus providing the provided content data is invalid based on the public key certificate revocation list distributed from the management apparatus, and controls the distribution of the provided content data to the data processing apparatus based on the result of the related verification.

[0087] Further, a data providing system of a 32nd aspect of the invention has a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus, wherein the management apparatus manages the operation of a data providing service by the data providing apparatus, the data distribution apparatus, and the data processing apparatus, generates signature data indicating that the related data is generated by an apparatus itself by using its own secret key data when the data distribution apparatus supplies data to another apparatus, generates and manages public key certificate data of public key data corresponding to the secret key data of the data distribution apparatus for when another apparatus verifies the legitimacy of the related signature data by using the public key data corresponding to the secret key data, generates a public key certificate revocation list for specifying public key certificate data to be invalidated among the generated public key certificate data, and distributes the related public key certificate revocation list to the data providing apparatus, the data providing apparatus verifies whether or not public key certificate data of the data distribution apparatus of the destination of provision of the content data is invalid and controls the provision of the content data to the data distribution apparatus based on the result of the related verification, the data distribution apparatus distributes the provided content data to the data processing apparatus, and the data processing apparatus uses the distributed content data.

[0088] Further, a data providing system of a 33rd aspect of the invention has a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus, wherein the management apparatus manages the operation of a data providing service by the data providing apparatus, the data distribution apparatus, and the data processing apparatus, generates signature data indicating that the related data is generated by an apparatus itself by using its own secret key data when the data distribution apparatus supplies data to another apparatus, generates and manages public key certificate data of public key data corresponding to the secret key data of the data distribution apparatus for when another apparatus verifies the legitimacy of the related signature data by using the public key data corresponding to the secret key data, generates a public key certificate revocation list for specifying public key certificate data to be invalidated among the generated public key certificate data, and distributes the related public key certificate revocation list to the data distribution apparatus, the data providing apparatus provides content data to the data distribution apparatus, the data distribution apparatus distributes the provided content data and the distributed public key certificate revocation list to the data processing apparatus, and the data processing apparatus verifies whether or not public key certificate data of the data distribution apparatus distributing the distributed content data is invalid based on the distributed public key certificate revocation list and controls the usage of the distributed content data based on the result of the related verification.

[0089] Further, a data providing system of a 34th aspect of the invention has a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus, wherein the management apparatus manages the operation of a data providing service by the data providing apparatus, the data distribution apparatus, and the data processing apparatus, generates signature data indicating that the related data is generated by an apparatus itself by using its own secret key data when the data distribution apparatus supplies data to another apparatus, generates and manages public key certificate data of public key data corresponding to the secret key data of the data distribution apparatus for when another apparatus verifies the legitimacy of the related signature data by using public key data corresponding to the secret key data, generates a public key certificate revocation list for specifying public key certificate data to be invalidated among the generated public key certificate data, and distributes the related public key certificate revocation list to the data processing apparatus, the data providing apparatus provides content data to the data distribution apparatus, the data distribution apparatus distributes the provided content data to the data processing apparatus, and the data processing apparatus verifies whether or not public key certificate data of the data distribution apparatus distributing the distributed content data is invalid based on the distributed public key certificate revocation list and controls the usage of the distributed content data based on the result of the related verification.

[0090] Further, a data providing system of a 35th aspect of the invention has a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus, wherein the management apparatus manages the operation of a data providing service by the data providing apparatus, the data distribution apparatus, and the data processing apparatus, generates signature data indicating that the related data is generated by an apparatus itself by using its own secret key data when the data distribution apparatus supplies data to another apparatus, generates and manages public key certificate data of public key data corresponding to the secret key data of the data distribution apparatus for when another apparatus verifies the legitimacy of the related signature data by using public key data corresponding to the secret key data, generates a public key certificate revocation list for specifying public key certificate data to be invalidated among the generated public key certificate data, and distributes the related public key certificate revocation list to the data providing apparatus, the data providing apparatus provides content data and the public key certificate revocation list to the data distribution apparatus, the data distribution apparatus distributes the provided content data and public key certificate revocation list to the data processing apparatus, and the data processing apparatus verifies whether or not public key certificate data of the data distribution apparatus distributing the distributed content data is invalid based on the distributed public key certificate revocation list and controls the usage of the distributed content data based on the result of the related verification.

[0091] Further, a data providing system of a 36th aspect of the invention has a data providing apparatus, data distribution apparatus, a plurality of data processing apparatuses, and a management apparatus, wherein the management apparatus manages the operation of a data providing service by the data providing apparatus, the data distribution apparatus, and the data processing apparatuses, generates signature data indicating that the related data is generated by an apparatus itself by using its own secret key data when a data processing apparatus supplies data to another apparatus, generates and manages public key certificate data of public key data corresponding to the secret key data of the data processing apparatuses for when another apparatus verifies the legitimacy of the related signature data by using the public key data corresponding to the secret key data, generates a public key certificate revocation list for specifying public key certificate data to be invalidated among the generated public key certificate data, and distributes the related public key certificate revocation list to the data providing apparatus, the data providing apparatus provides content data and the public key certificate revocation list to the data distribution apparatus, the data distribution apparatus distributes the provided content data and a public key certificate revocation list to the data processing apparatuses, and the data processing apparatuses verify whether or not public key certificate data of the other data processing apparatuses are invalid based on the public key certificate revocation list distributed from the data distribution apparatus and control the communication with other data processing apparatuses based on the result of the related verification.

[0092] Further, a data providing system of a 37th aspect of the invention has a data providing apparatus, data distribution apparatus, a plurality of data processing apparatuses, and a management apparatus, wherein the management apparatus manages the operation of a data providing service by the data providing apparatus, the data distribution apparatus, and the data processing apparatuses, generates signature data indicating that the related data is generated by an apparatus itself by using its own secret key data when a data processing apparatus supplies data to another apparatus, generates and manages public key certificate data of public key data corresponding to the secret key data of the data processing apparatuses for when another apparatus verifies the legitimacy of the related signature data by using the public key data corresponding to the secret key data, generates a public key certificate revocation list for specifying public key certificate data to be invalidated among the generated public key certificate data, and distributes the related public key certificate revocation list to the data providing apparatus, the data providing apparatus provides content data to the data distribution apparatus, the data distribution apparatus distributes the provided content data and the distributed public key certificate revocation list to the data processing apparatuses, and the data processing apparatuses verify whether or not public key certificate data of other data processing apparatuses are invalid based on the public key certificate revocation list distributed from the data distribution apparatus, and control the communication with other data processing apparatuses based on the result of the related verification.

[0093] Further, a data providing system of a 38th aspect of the invention has a data providing apparatus, data distribution apparatus, a plurality of data processing apparatuses, and a management apparatus, wherein a data processing apparatus supplies registration data, indicating an already registered data processing apparatus connected in a predetermined network to which is connected, to the management apparatus, refers to a revocation flag in registration data supplied from the management apparatus and restricts communication with another data processing apparatus having public key certificate data indicated as invalid by the revocation flag, the management apparatus manages the operation of a data providing service by the data providing apparatus, the data distribution apparatus, and the data processing apparatuses, generates and manages public key certificate data of public key data corresponding to the secret key data for when a data processing apparatus generates signature data indicating legitimacy of

data using its own secret key data when supplying data to another apparatus, generates a public key certificate revocation list for specifying public key certificate data to be invalidated among the generated public key certificate data, stores the related public key certificate revocation list, generates new registration data by setting the revocation flag in the registration data supplied from data processing apparatuses based on the related public key certificate revocation list, and distributes the related generated registration data to the data processing apparatuses, the data providing apparatus provides content data to the data distribution apparatus, and the data distribution apparatus distributes the provided content data to the data processing apparatuses.

[0094] Further, a data providing system of a 39th aspect of the invention has a data providing apparatus, data distribution apparatus, a plurality of data processing apparatuses, and a management apparatus, wherein the management apparatus manages the operation of a data providing service by the data providing apparatus, the data distribution apparatus, and the data processing apparatuses, generates and manages public key certificate data of public key data corresponding to the secret key data for when a data processing apparatus generates signature data indicating the legitimacy of data by using its own secret key data when supplying the related data to another apparatus, generates a public key certificate revocation list for specifying public key certificate data to be invalidated among the generated public key certificate data, and distributes the related public key certificate revocation list to the data providing apparatus, the data providing apparatus provides content data and the public key certificate revocation list to the data distribution apparatus, the data distribution apparatus distributes the provided content data and the public key certificate revocation list to the data processing apparatuses, and a data processing apparatus sets a revocation flag in registration data indicating an already registered data processing apparatus connected in a predetermined network to which it is connected based on the distributed public key certificate revocation list and restricts communication with another data processing apparatus having public key certificate data indicated as invalid by the related revocation flag.

[0095] Further, a data providing system of a 40th aspect of the invention has a data providing apparatus, data distribution apparatus, a plurality of data processing apparatuses, and a management apparatus, wherein the management apparatus manages the operation of a data providing service by the data providing apparatus, the data distribution apparatus, and the data processing apparatuses, generates and manages public key certificate data of public key data corresponding to the secret key data for when a data processing apparatus generates signature data indicating the legitimacy of the data by using its own secret key data when supplying the related data to another apparatus, generates a public key certificate revocation list for specifying public key certificate data to be invalidated among the generated public key certificate data, and distributes the related public key certificate revocation list to the data distribution apparatus, the data providing apparatus provides content data to the data distribution apparatus, the data distribution apparatus distributes the provided content data and the public key certificate revocation list to the data processing apparatuses, and a data processing apparatus sets a revocation flag in registration data indicating an already registered data processing apparatus connected in a predetermined network to which it is connected based on the distributed public key certificate revocation list and restricts communication with another data processing apparatus having public key certificate data indicated as invalid by the related revocation flag.

[0096] Further, a data providing system of a 41st aspect of the invention is a data providing system comprising a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus, wherein the data providing apparatus provides content data and usage control policy data indicating the handling of the related content data to the data distribution apparatus, the data distribution apparatus distributes the provided content data and the usage control policy data to the data processing apparatus, the data processing apparatus has a first module for communicating with the data distribution apparatus and a second module for determining at least one of a purchase mode and usage mode of the distributed content data based on the distributed usage control policy data and transmitting log data indicating the log of the related determined purchase mode and usage mode to the management apparatus, the management apparatus manages the data providing apparatus, data distribution apparatus, and data processing apparatus and has a settlement function for performing profit distribution processing for distributing the profit obtained accompanied with the data processing apparatus receiving distribution of the content data and purchasing and using the content data to related parties of the data providing apparatus and the data distribution apparatus based on the log data received from the second module and performing settlement based on the result of the related profit distribution processing and a right management function for registering the usage control policy data.

[0097] Further, a data providing system of a 42nd aspect of the invention is a data providing system comprising a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus, wherein the data providing apparatus provides content data and usage control policy data indicating the handling of the related content data to the data distribution apparatus, the data distribution apparatus has a charging function for performing settlement processing by using settlement claim data distributed from the management apparatus and distributes the provided content data and the usage control policy data to the data processing apparatus, the data processing apparatus

has a first module for communicating with the data distribution apparatus and a second module for determining at least one of a purchase mode and usage mode of the distributed content data based on the distributed usage control policy data and transmitting log data indicating the log of the related determined purchase mode and usage mode to the management apparatus, the management apparatus manages the data providing apparatus, data distribution apparatus, and data processing apparatus and has a settlement claim data creation function for performing profit distribution processing for distributing the profit obtained accompanied with the data processing apparatus receiving distribution of the content data and purchasing and using the content data to related parties of the data providing apparatus and the data distribution apparatus based on the log data received from the second module, creating settlement claim data used when performing settlement based on the result of the related profit distribution processing, and supplying the same to the data distribution apparatus and a right management function for registering the usage control policy data.

[0098] Further, a data providing system of a 43rd aspect of the invention is a data providing system comprising a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus, wherein the data providing apparatus has a charging function for performing settlement processing by using settlement claim data distributed from the management apparatus and provides content data and usage control policy data indicating the handling of the related content data to the data distribution apparatus, the data distribution apparatus distributes the provided content data and the usage control policy data to the data processing apparatus, the data processing apparatus has a first module for communicating with the data distribution apparatus and a second module for determining at least one of a purchase mode and usage mode of the distributed content data based on the distributed usage control policy data and transmitting log data indicating the log of the related determined purchase mode and usage mode to the management apparatus, the management apparatus manages the data providing apparatus, data distribution apparatus, and data processing apparatus and has a settlement claim data creation function for performing profit distribution processing for distributing the profit obtained accompanied with the data processing apparatus receiving the distribution of the content data and purchasing and using the content data to related parties of the data providing apparatus and the data distribution apparatus based on the log data received from the second module, creating settlement claim data used when performing settlement based on the result of the related profit distribution processing, and distributing the same to the data providing apparatus and a right management function for registering the usage control policy data.

[0099] Further, a management apparatus of a 44th aspect of the invention is a management apparatus for managing a data providing apparatus for distributing content data and usage control policy data indicating the handling of the related content data and a data processing apparatus for determining at least one of a purchase mode and a usage mode of the distributed content data based on the distributed usage control policy data and creating log data indicating the log of at least one of the related determined purchase mode and usage mode and receives the log data from the data processing apparatus and performs profit distribution processing for distributing the profit obtained accompanied with the purchase and the usage of the content data in the data processing apparatus to related parties of the data providing apparatus based on the related received log data.

[0100] Further, a management apparatus of a 45th aspect of the invention is a management apparatus for managing a data providing apparatus for providing content data and usage control policy data indicating the handling of the related content data, a data distribution apparatus for distributing the provided content data and the usage control policy data, and a data processing apparatus for determining at least one of a purchase mode and usage mode of the distributed content data based on the distributed usage control policy data and creating log data indicating the log of at least one of the related determined purchase mode and usage mode and performs profit distribution processing for distributing the profit obtained accompanied with the data processing apparatus receiving the distribution of the content data and purchasing and using the content data to related parties of the data providing apparatus and the data distribution apparatus based on the received log data.

[0101] Further, a data processing apparatus of a 46th aspect of the invention is a data processing apparatus for receiving distribution of content data and usage control policy data indicating the handling of the related content data from a data providing apparatus and transmitting the log data to a management apparatus for performing profit distribution processing for distributing the profit obtained accompanied with the purchase and usage of the related distributed content data to related parties of the data providing apparatus based on the predetermined log data, determines at least one of a purchase mode and usage mode of the distributed content data based on the distributed usage control policy data, and transmits the log data indicating the log of the determined designation mode and usage mode to the management apparatus.

[0102] Further, a data processing apparatus of a 47th aspect of the invention is a data processing apparatus for receiving distribution of content data and usage control policy data from a data distribution apparatus receiving the provision of content data and usage control policy data indicating the handling of the related content data from a data providing apparatus and transmitting log data to a management apparatus for performing profit distribution processing for distributing the profit

obtained accompanied with the purchase and usage of the distributed content data to related parties of the data providing apparatus and the data distribution apparatus based on predetermined log data and has a first module for communicating with the data distribution apparatus and a second module for determining at least one of a purchase mode and usage mode of the distributed content data based on the distributed usage control policy data and transmitting log data indicating the log of the related determined purchase mode and usage mode to the management apparatus.

[0103] Further, a data processing apparatus of a 48th aspect of the invention is a data processing apparatus for receiving the distribution of content data and usage control policy data indicating the handling of the related content data from a data providing apparatus via a data distribution apparatus and transmitting the log data to a management apparatus for performing profit distribution processing for distributing the profit obtained accompanied with the purchase and usage of the related distributed content data to related parties of the data providing apparatus and the data distribution apparatus based on the management apparatus use log data and has a first module for creating data distribution apparatus use purchase log data indicating the log of the purchase of the content data distributed from the data distribution apparatus and transmitting the same to the data distribution apparatus and a second module for determining at least one of a purchase mode and usage mode of the distributed content data based on the distributed usage control policy data and transmitting the management apparatus use log data indicating the log of the related determined purchase mode and usage mode to the management apparatus.

[0104] Further, a data providing method of a 49th aspect of the invention is a data providing method using a data providing apparatus, data processing apparatus, and management apparatus comprising the steps of distributing content data and usage control policy data indicating the handling of the related content data from the data providing apparatus to the data processing apparatus, having the data processing apparatus determine at least one of the purchase mode and the usage mode of the distributed content data based on the distributed usage control policy data and transmitting log data indicating the log of at least one of the related determined purchase mode and usage mode to the management apparatus, and having the management apparatus perform profit distribution processing for distributing the profit obtained accompanied with the purchase and the usage of the content data in the data processing apparatus to related parties of the data providing apparatus based on the received log data.

[0105] Further, a data providing method of a 50th aspect of the invention is a data providing method using a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus comprising the steps of providing content data and usage control policy data indicating the handling of the related content data from the data providing apparatus to the data distribution apparatus, distributing the provided content data and the usage control policy data from the data distribution apparatus to the data processing apparatus, having the data processing apparatus determine at least one of the purchase mode and the usage mode of the distributed content data based on the distributed usage control policy data and transmitting log data indicating the log of the related determined purchase mode and usage mode to the management apparatus, and having the management apparatus perform profit distribution processing for distributing the profit obtained accompanied with the data processing apparatus receiving the distribution of the content data and purchasing and using the content data to related parties of the data providing apparatus and the data distribution apparatus based on the log data received from the second module.

[0106] Further, a data providing method of a 51st aspect of the invention is a data providing method using a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus comprising the steps of providing content data and usage control policy data indicating the handling of the related content data from the data providing apparatus to the data distribution apparatus, distributing the content data and the usage control policy data provided from the data distribution apparatus to the data processing apparatus to the data processing apparatus, having the data processing apparatus generate data distribution apparatus use purchase log data indicating the log of the purchase of the content data distributed from the data distribution apparatus and transmitting the same to the data distribution apparatus, determine at least one of a purchase mode and usage mode of the distributed content data based on the distributed usage control policy data, and transmit management apparatus use log data indicating the log of the related determined purchase mode and usage mode to the management apparatus, having the management apparatus clear the profit obtained accompanied with the purchase and the usage of the content data in the data processing apparatus to related parties of the data providing apparatus and the data distribution apparatus based on the management apparatus use log data, and having the data distribution apparatus perform charging processing concerning the distribution of the content data based on the data distribution apparatus use purchase log data received from the data processing apparatus.

BRIEF DESCRIPTION OF THE DRAWINGS

[0107] Figure 1 is a view of the overall configuration of an EMD system of a first embodiment of the present invention.

[0108] Figure 2 is a functional block diagram of a content provider shown in Fig. 1 and a view of the flow of

data concerning data transferred with a SAM of a user home network.

[0109] Figure 3 is a functional block diagram of the content provider shown in Fig. 1 and a view of the flow of the data concerning the data transferred between the content provider and an EMD service center.

[0110] Figure 4 is a view for explaining a format of a secure container transmitted from the content provider shown in Fig. 1 to a SAM.

[0111] Figure 5 is a view for explaining a correspondence between an OSI layer and a definition of the secure container of the present embodiment.

[0112] Figure 6 is a view for explaining a ROM type storage medium.

[0113] Figure 7A is a view for explaining a format of a right registration request use module transmitted from the content provider to the EMD service center, while Fig. 7B is a view for explaining an authorization certificate module transmitted from the EMD service center to the content provider.

[0114] Figure 8 is a flowchart of processing where the content provider requests public key certificate data for certifying legitimacy of public key data corresponding to its own secret key data to the EMD service center in the first embodiment.

[0115] Figure 9 is a flowchart of processing where the content provider transmits a secure container to a SAM of the user home network in the first embodiment.

[0116] Figure 10 is a functional block diagram of the EMD service center shown in Fig. 1 and a view of the flow of the data related to the data transferred with the content provider.

[0117] Figure 11 is a functional block diagram of the EMD service center shown in Fig. 1 and a view of the flow of the data related to the data transferred between a SAM and a settlement organization shown in Fig. 1.

[0118] Figure 12 is a flowchart of processing where the EMD service center receives a request for issuance of public key certificate data from the content provider in the first embodiment.

[0119] Figure 13 is a flowchart of processing where the EMD service center receives a request for issuance of public key certificate data from a SAM in the first embodiment.

[0120] Figure 14 is a flowchart of processing where the EMD service center receives a request for registration of usage control policy data and content key data from the content provider in the first embodiment.

[0121] Figure 15 is a flowchart of processing where the EMD service center performs settlement processing in the first embodiment.

[0122] Figure 16 is a view of the configuration of a network apparatus in the user home network shown in Fig. 1.

[0123] Figure 17 is a functional block diagram of a SAM in the user home network shown in Fig. 1 and a view of the flow of the data up to decryption of the secure container received from the content provider.

[0124] Figure 18 is a view for explaining the data stored in an external memory shown in Fig. 16.

[0125] Figure 19 is a view for explaining the data stored in a stack memory.

[0126] Figure 20 is another view of the configuration of the network apparatus in the user home network shown in Fig. 1.

[0127] Figure 21 is a view for explaining the data stored in a storage unit shown in Fig. 17.

[0128] Figure 22 is a flowchart of processing in a SAM when inputting the secure container from the content provider and decrypting a key file KF in the secure container in the first embodiment.

[0129] Figure 23 is a functional block diagram of a SAM in the user home network shown in Fig. 1 and a view of the flow of the data related to the processing of using and purchasing the content data.

[0130] Figure 24 is a flowchart of processing up to determination of a purchase mode of the secure container downloaded from the content provider in a download memory in the first embodiment.

[0131] Figure 25 is a flowchart of processing in the case of reproduction of content data with the purchase mode already determined stored in the download memory in the first embodiment.

[0132] Figure 26 is a view for explaining the flow of the processing in a SAM of the source of transfer when transferring a content file with the purchase mode already determined downloaded in the download memory of the network apparatus shown in Fig. 16 to a SAM of an AV apparatus.

[0133] Figure 27 is a view of the flow of the data in a SAM of the source of transfer in the case shown in Fig. 26.

[0134] Figure 28 is a flowchart of the processing in a SAM when transferring the content file and the key file with the purchase mode already determined therein downloaded in the download memory of the network apparatus to a SAM of another AV apparatus in the first embodiment.

[0135] Figure 29 is a view for explaining the format of a secure container with the purchase mode already determined.

[0136] Figure 30 is a view of the flow of the data when writing an input content file etc. into a RAM type or ROM type storage medium in the SAM of the source of transfer in the case shown in Fig. 26.

[0137] Figure 31 is a flowchart of the processing in the SAM when writing a content file input from another SAM etc. into a storage medium of a RAM type or the like in the first embodiment.

[0138] Figure 32 is a view for explaining the flow of the processing when determining the purchase mode in an AV apparatus when the user home network receives off-line the distribution of the ROM type storage medium shown in Fig. 6 wherein the purchase mode of the content has not yet been determined.

[0139] Figure 33 is a view of the flow of the data in a

SAM in the case shown in Fig. 32.

[0140] Figure 34 is a flowchart of processing when determining the purchase mode in an AV apparatus when the user home network receives off-line the distribution of the ROM type storage medium shown in Fig. 5 wherein the purchase mode of the content has not yet been determined in the first embodiment.

[0141] Figure 35 is a flowchart continuing from the flowchart of Fig. 34.

[0142] Figure 36 is a view for explaining the flow of processing when reading a secure container from a ROM type storage medium wherein the purchase mode of the content has not yet been determined in an AV apparatus in the user home network, transferring this to another AV apparatus, and writing the same into a RAM type storage medium.

[0143] Figure 37 is a flowchart of processing of a first AV apparatus when reading a secure container from a ROM type storage medium wherein the purchase mode of the content has not yet been determined in a first AV apparatus as shown in Fig. 36, transferring this to a second AV apparatus, determining the purchase mode in the second AV apparatus, and writing the same into a RAM type storage medium.

[0144] Figure 38 is a flowchart of the processing of the second AV apparatus of the case shown in Fig. 37.

[0145] Figure 39 is a flowchart continuing from the flowchart shown in Fig. 38.

[0146] Figure 40 is a view of the flow of the data in the SAM of the source of transfer in the case shown in Fig. 36.

[0147] Figure 41 is a view of the flow of the data in the SAM of the source of transfer in the case shown in Fig. 36.

[0148] Figure 42 is a view for explaining the format of the data transferred by an in-band method and an out-of-band method among the content provider, EMD service center, and SAM shown in Fig. 1.

[0149] Figure 43 is a view for explaining the mode of the data transferred by the in-band method and the out-of-band method among the content provider, EMD service center, and SAM shown in Fig. 1.

[0150] Figure 44 is a view for explaining an example of a connection configuration of apparatuses to a bus.

[0151] Figure 45 is a view for explaining a data format of a SAM registration list.

[0152] Figure 46 is a flowchart of the overall operation of the content provider shown in Fig. 1.

[0153] Figure 47 is a view for explaining a second modification of the first embodiment of the present invention.

[0154] Figure 48 is a view for explaining a third modification of the first embodiment of the present invention.

[0155] Figure 49 is a view of the overall configuration of the EMD system of a second embodiment of the present invention.

[0156] Figure 50 is a functional block diagram of the content provider shown in Fig. 49 and a view of the flow of the data related to the secure container transmitted to a service provider.

[0157] Figure 51 is functional block diagram of the service provider shown in Fig. 49 and a view of the flow of the data transferred with the user home network.

[0158] Figure 52 is a flowchart of the processing of the service provider when preparing a secure container from a secure container supplied from the content provider and distributing this to the user home network in the second embodiment.

[0159] Figure 53 is a view for explaining the mode of the secure container transmitted from the service provider shown in Fig. 49 to the user home network.

[0160] Figure 54 is a functional block diagram of the service provider shown in Fig. 49 and a view of the flow of the data transferred with the EMD service center.

[0161] Figure 55 is a view for explaining the format of a price tag registration request use module transmitted from the service provider to the EMD service center.

[0162] Figure 56 is a functional block diagram of the EMD service center shown in Fig. 49 and a view of the flow of the data related to the data transferred with the service provider.

[0163] Figure 57 is a functional block diagram of the EMD service center shown in Fig. 49 and a view of the flow of the data related to the data transferred with the content provider.

[0164] Figure 58 is a functional block diagram of the EMD service center shown in Fig. 49 and a view of the flow of the data related to the data transferred with the SAM.

[0165] Figure 59 is a view for explaining the content of a usage log data.

[0166] Figure 60 is a flowchart of processing when the EMD service center receives a request for issuance of public key certificate data from the service provider in the second embodiment.

[0167] Figure 61 is a flowchart of processing when the EMD service center receives a request for registration of price tag data from the service provider in the second embodiment.

[0168] Figure 62 is a flowchart of processing when the EMD service center performs settlement in the second embodiment.

[0169] Figure 63 is a view of the configuration of the network apparatus shown in Fig. 49.

[0170] Figure 64 is a functional block diagram of a CA module shown in Fig. 63.

[0171] Figure 65 is a functional block diagram of the SAM shown in Fig. 63 and a view of the flow of the data from the input of the secure container to the decryption of the same.

[0172] Figure 66 is a view for explaining the data stored in the storage unit shown in Fig. 65.

[0173] Figure 67 is a functional block diagram of the SAM shown in Fig. 63 and a view of the flow of the data when determining the purchase and/or usage mode of the content etc.

[0174] Figure 68 is a flowchart of processing of the SAM when inputting a secure container from the service provider and decrypting the key file in the secure container in the second embodiment.

[0175] Figure 69 is a flowchart of processing of the SAM up to the determination of the purchase mode of the secure container downloaded in the download memory from the service provider in the second embodiment.

[0176] Figure 70 is a flowchart of processing when reproducing content data having the purchase mode already determined stored in the download memory.

[0177] Figure 71 is a view for explaining the mode of the key file after the purchase mode is determined.

[0178] Figure 72 is a view for explaining the flow of the processing in the SAM of the source of transfer when transferring the content file having the purchase mode already determined downloaded in the download memory of the network apparatus shown in Fig. 63 to the SAM of the AV apparatus.

[0179] Figure 73 is a view of the flow of the data in the SAM of the source of transfer in the case shown in Fig. 72.

[0180] Figure 74 is a flowchart of processing of the SAM of the source of transfer in a case when transferring for example the content file having the purchase mode already determined downloaded in the download memory of the network apparatus to the SAM of the AV apparatus as shown in Fig. 72.

[0181] Figure 75 is a view for explaining the format of the secure container having the purchase mode already determined to be transferred to the SAM of the AV apparatus from the SAM of the network apparatus.

[0182] Figure 76 is a view of the flow of the data in the SAM of the destination of transfer in the case shown in Fig. 72.

[0183] Figure 77 is a flowchart of the processing of the SAM when writing a content file input from the other SAM etc. into a storage medium of the RAM type etc. as shown in Fig. 72.

[0184] Figure 78 is a flowchart of the overall operation of the EMD system shown in Fig. 49.

[0185] Figure 79 is a flowchart of the overall operation of the EMD system shown in Fig. 49.

[0186] Figure 80 is a view of the configuration of an EMD system using two service providers according to a first modification of the second embodiment of the present invention.

[0187] Figure 81 is a view of the configuration of an EMD system using a plurality of content providers according to a second modification of the second embodiment of the present invention.

[0188] Figure 82 is a view of the configuration of an EMD system according to a third modification of the second embodiment of the present invention.

[0189] Figure 83 is a view of the configuration of an EMD system according to a fourth modification of the second embodiment of the present invention.

[0190] Figure 84 is a view for explaining the mode of a route of acquisition of public key certificate data.

[0191] Figure 85 is a view for explaining processing for invalidating public key certificate data of the content provider.

[0192] Figure 86 is a view for explaining processing for invalidating public key certificate data of the service provider.

[0193] Figure 87 is a view for explaining processing for invalidating public key certificate data of a SAM.

[0194] Figure 88 is a view for explaining other processing for invalidating public key certificate data of a SAM.

[0195] Figure 89 is a view for explaining a case where a right management clearing house and an electronic settlement clearing house are provided in place of the EMD service center in the EMD system shown in Fig. 49.

[0196] Figure 90 is a view of the configuration of an EMD system when providing the right management clearing house and the electronic settlement clearing house shown in Fig. 89 in a single EMD service center.

[0197] Figure 91 is a view of the configuration of an EMD system where the service provider directly performs settlement at the electronic settlement clearing house.

[0198] Figure 92 is a view of the configuration of an EMD system where the content provider directly performs the settlement at the electronic settlement clearing house.

[0199] Figure 93 is a view for explaining the format of the secure container provided from the content provider to the service provider shown in Fig. 49 in an eighth modification of the second embodiment of the present invention.

[0200] Figure 94 is a view for explaining a detailed format of a module stored in Fig. 93.

[0201] Figure 95 is a view for explaining the format of the secure container provided from the service provider to the SAM shown in Fig. 49 in the eighth modification of the second embodiment of the present invention.

[0202] Figure 96 is a conceptual view of a case where the secure container is provided by using the Internet.

[0203] Figure 97 is another conceptual view of the case where the secure container is provided by using the Internet.

[0204] Figure 98 is a conceptual view of a case where the secure container is provided by using a digital broadcast.

[0205] Figure 99 is another conceptual view of the case where the secure container is provided by using a digital broadcast.

[0206] Figure 100 is a view of the configuration of a conventional EMD system.

BEST MODE FOR WORKING THE INVENTION

[0207] Below, an explanation will be made of an EMD (electronic music distribution) system according to embodiments of the present invention.

[0208] In the present embodiment, the content data distributed to the user means digital data wherein the information per se has value such as music data, video data, and a program. The explanation will be made below by taking as an example music data.

First Embodiment

[0209] Figure 1 is a view of the configuration of an EMD system 100 of the present embodiment.

[0210] As shown in Fig. 1, the EMD system 100 has a content provider 101, an EMD service center (clearing house, below, also described as "ESC") 102, and a user home network 103.

[0211] Here, the content provider 101, EMD service center 102, and SAMs 105_1 to 105_4 correspond to the data providing apparatus, management apparatus, and data processing apparatuses of the present invention.

[0212] First, a brief explanation will be made of the EMD system 100.

[0213] In the EMD system 100, the content provider 101 transmits usage control policy (UCP) data 106 indicating the content of the right such as license conditions of content data C of the content which it is to provide to the EMD service center 102 as a high reliability authority manager. The usage control policy data 106 is authorized (certified) by the EMD service center 102.

[0214] Further, the content provider 101 encrypts the content data C by content key data Kc to generate a content file CF and, at the same time, encrypts the content key data Kc by distribution key data KD_1 to $KD5_8$ of a corresponding period distributed from the EMD service center 102. Then, the content provider 101 distributes a secure container (module of the present invention) 104 storing (encapsulating) the encrypted content key data Kc and content file CF and its own signature data to the user home network 103 by using a network such as the Internet, digital broadcasting, and storage medium.

[0215] In this way, in the present embodiment, by encapsulating and providing the digital content data C, the digital content which had been closely tied to a conventional storage medium is separated from the storage medium, thus value can be imparted to the digital content by itself.

[0216] Here, the "secure container" is the product capsule forming the most basic unit when selling the content data C (product) no matter which distribution route (distribution channel) it is provided through. Specifically, the secure container is a product capsule containing the encryption information for the charging, signature data for verifying the legitimacy of the content of the content data C, the legitimacy of the party preparing the content data, and the legitimacy of the distributor of the content data, and the information relating to the copyright such as the information concerning the electronic watermark information buried in the content data.

[0217] The user home network 103 has for example a network apparatus 160_1 and AV apparatuses 160_2 to 160_4.

[0218] The network apparatus 160_1 includes a SAM (secure application module) 105_1.

[0219] The AV apparatuses 160_2 to 160_4 include the SAMs 105_2 to 105_4. The SAMs 105_1 to 105_4 are connected to each other via a bus 191, for example, an IEEE (Institute of Electrical and Electronics Engineers) 1394 serial interface bus.

[0220] The SAMs 105_1 to 105_4 decrypt the secure container 104 received by the network apparatus 160_1 from the content provider 101 via the network or the like on-line and/or the secure container 104 received from the content provider 101 at the AV apparatuses 160_2 to 160_4 via storage media off-line by using the distribution key data KD_1 to KD_3 of the corresponding period and then verify the signature data.

[0221] The secure container 104 supplied to the SAMs 105_1 to 105_4 is reproduced or stored to a storage medium after the purchase and/or usage mode is determined in accordance with the operation of the user in the network apparatus 160_1 and the AV apparatuses 160_2 to 160_4.

[0222] The SAM 105_1 to 105_4 store logs of the purchase and/or usage of the secure container 104 mentioned above as usage log data 108.

[0223] The usage log data 108 is transmitted from the user home network 103 to the EMD service center 102 in response to for example a request from the EMD service center 102.

[0224] The EMD service center 102 determines (calculates) the charged content based on the usage log data 108 and performs settlement at a settlement organization 91 such as a bank via a payment gateway 90. By this, the money paid by a user of the user home network 103 to the settlement organization 91 is paid to the content provider 101 by the settlement processing by the EMD service center 102.

[0225] Further, the EMD service center 102 transmits a settlement report data 107 to the content provider 101 every predetermined period.

[0226] In the present embodiment, the EMD service center 102 has a certificate authority function, a key data management function, and a right clearing (profit distribution) function.

[0227] Namely, the EMD service center 102 plays the role as a second certificate authority with respect to a route certificate authority 92 constituting the highest authority manager at a neutral position (located below the route certificate authority 92) and certifies the legitimacy of the related public key data by attaching a signature using the secret key data of the EMD service center 102 to public key certificate data of public key data used for the verification processing of the signature data in the content provider 101 and the SAMs 105_1 to 105_4. Further, as mentioned before, one of the certificate authority functions of the EMD service center 102 is for the EMD service center 102 to register and authorize the usage

control policy data 106 of the content provider 101.

[0228] Further, the EMD service center 102 has a key data management function for managing the key data, for example, the distribution key data KD_1 to KD_6.

[0229] Further, the EMD service center 102 has a right clearing (profit distribution) function of performing settlement with respect to the purchase and/or usage of content by a user based on a suggested retailer's price (SRP) described in the authorized usage control policy data 106 and the usage log data 108 input from the SAMs 105_1 to 105_4 and distributing the money paid by the user to the content provider 101.

[0230] Below, a detailed explanation will be made of components of the content provider 101.

[Content Provider 101]

[0231] Figure 2 is a functional block diagram of the content provider 101 and shows the flow of the data related to the data transferred with the SAMs 105_1 to 105_4 of the user home network 103.

[0232] Further, in Fig. 3, the flow of the data related to the data transferred between the content provider 101 and the EMD service center 102 is shown.

[0233] Note that, in the figures starting from Fig. 3, the flow of the data input and output to and from the signature data processor and the encryptor/decryptor using session key data K_{SES} is omitted.

[0234] As shown in Fig. 2 and Fig. 3, the content provider 101 has a content master source server 111, an electronic watermark information adder 112, a compressor 113, an encryptor 114, a random number generator 115, an encryptor 116, a signature processor 117, a secure container generator 118, a secure container database 118a, a storage unit 119, a mutual authenticator 120, an encryptor/decryptor 121, a usage control policy data generator 122, a SAM manager 124, and an EMD service center manager 125.

[0235] The content provider 101 registers for example public key data generated by itself and its own ID card and bank account number (account number for settlement) in the EMD service center 102 off-line before communicating with the EMD service center 102 and acquires its own identifier (identification number) CP_ID. Further, the content provider 101 receives public key data of the EMD service center 102 and public key data of the route certificate authority 92 from the EMD service center 102.

[0236] Below, an explanation will be made of functional blocks of the content provider 101 shown in Fig. 2 and Fig. 3.

[0237] The content master server 111 stores the content data of the master source of content to be provided to the user home network 103 and outputs content data S111 to be provided to the electronic watermark information adder 112.

[0238] The electronic watermark information adder 112 buries a source watermark Ws, a copy control watermark Wc, a user watermark Wu, etc. in the content data S111 to generate content data S112 and outputs the content data S112 to the compressor 113.

[0239] The source watermark Ws is information concerning the copyright such as the name of the owner of the copyright of the content data, ISRC code, authoring date, authoring apparatus ID (identification data), and destination of the distribution of the content. The copy control watermark Wc is information containing a copy prohibit bit for preventing copying through an analog interface. The user watermark Wu contains for example the identifier CP_ID of the content provider 101 for specifying a source of distribution and a destination of distribution of the secure container 104 and identifiers SAM_ID_1 to SAM_ID_4 of the SAMs 105_1 to 105_4 of the user home network 103.

[0240] Further, the electronic watermark information adder 112 buries the link use ID for searching of the content data by a search engine as electronic watermark information in the content data S111 if necessary.

[0241] In the present embodiment, preferably the information content and the burial position of each electronic watermark information are defined as the electronic watermark information management data. The electronic watermark information management data is managed in the EMD service center 102. The electronic watermark information management data is used when for example the network apparatus 160_1 and the AV apparatuses 160_2 to 160_4 in the user home network 103 verify the legitimacy of the electronic watermark information.

[0242] For example, in the user home network 103, based on the electronic watermark information management data, the burying of a false electronic watermark information can be detected with a high probability by deciding that the electronic watermark information is legitimate when both of the burial position of the electronic watermark information and the content of the buried electronic watermark information coincide.

[0243] The compressor 113 compresses the content data S112 by an audio compression method such as ATRAC3 (Adaptive Transform Acoustic Coding 3) (trademark) and outputs compressed content data S113 to the encryptor 114.

[0244] The encryptor 114 uses the content key data Kc as a common key, encrypts the content data S113 by a common key encryption method such as DES (Data Encryption Standard) or Triple DES to generate the content data C and outputs this to the secure container generator 118.

[0245] Further, the encryptor 114 encrypts A/V decompression software Soft and meta-data Meta by using the content key data Kc as the common key, then outputs the same to the secure container generator 117.

[0246] DES is an encryption method for processing 64 bits of a plain text as a block by using a 56-bit common key. The DES processing is comprised by a portion for scrambling the plain text to transform the same to

encrypted text (data scrambler) and a portion for creating key (magnification key) data used in the data scrambler from the common key data (key processor). All algorithms of DES are disclosed, so the fundamental processing of the data scrambler will be briefly explained here.

[0247] First, 64 bits of the plain text are divided into an upper significant 32-bit H_0 and a lower significant 32-bit L_0. Using as input the 48-bit magnification key data K_1 supplied from the key processor and the lower significant 32-bit L_0, the output of an F function obtained by scrambling the lower significant 32-bit L_0 is calculated. The F function is comprised by two types of basic transformations of "substitution" for replacing the numerals by a predetermined rule and "transposition" for switching the bit positions by a predetermined rule. Next, an exclusive OR of the upper significant 32-bit H_0 and the output of the F function is calculated, and the result thereof is made L_1. Further, L_0 is made H_1.

[0248] Then, based on the upper significant 32-bit H_0 and the lower significant 32-bit L_0, the above processing is repeated 16 times. The thus obtained upper significant 32-bit H_{18} and lower significant 32-bit L_{18} are output as the encrypted text. The decryption is realized by performing the above procedure in the reverse direction by using the common key data used in the encryption.

[0249] The random number generator 115 generates a random number of predetermined number of bits and outputs the related random number as the content key data Kc to the encryptor 114 and the encryptor 116.

[0250] Note that it is also possible to generate the content key data Kc from the information concerning the music provided by the content data. The content key data Kc is updated for example every predetermined time.

[0251] The encryptor 116 receives as its inputs the distribution key data KD_1 to KD_6 of the corresponding period among the distribution key data KD_1 to KD_6 received from the EMD service center 102 and stored in the storage unit 119 as will be mentioned later, encrypts the content key data Kc, usage control policy data 106, SAM program download containers SDC_1 to SDC_3, and a signature certificate module Mod_1 shown in Fig. 4B by the DES or other common encryption method using the related distribution key data as a common key, then outputs them to the secure container generator 117.

[0252] In the signature certificate module Mod_1, as shown in Fig. 4B, signature data $SIG_{2,CP}$ to $SIG_{4,CP}$, a public key certificate CER_{CP} of public key data $K_{CP,P}$ of the content provider 101 and signature data $SIG_{1,ESC}$ of the EMD service center 102 with respect to the related certificate CER_{CP} are stored.

[0253] Further, the SAM program download containers SDC_1 to SDC_3 store download drivers used when downloading programs in the SAMs 105_1 to 105_4, a UCP-L (Label) R (Reader) indicating the syntax (grammar) of a usage control policy data (UCP) U106, and lock key data for locking or unlocking rewrite and erase operations of the storage units (flash ROMs) built in the SAMs 105_1 to 105_4 in units of blocks.

[0254] Note that the storage unit 119 is provided with various databases, for example, a database for storing public key certificate data, a database for storing distribution use data KD_1 to KD_6, and a database for storing the key file KF.

[0255] The signature processor 117 takes a hush value of the data to be signed and generates the signature data SIG thereof by using the secret key data $K_{CP,S}$ of the content provider 101.

[0256] Note that the "hush value" is generated by using the hush function. The hush function is a function for receiving as the input the data covered, compressing the related input data to data having a predetermined bit length, and outputting the same as a hush value. The hush function is characterized in that it is difficult to predict the input from the hush value (output), many bits of the hush value change when one bit of the data input to the hush function changes, and it is difficult to find input data having an identical hush value.

[0257] The secure container generator 118, as shown in Fig. 4A, generates the content file CF storing header data and the content data C, A/V decompression software Soft, and meta-data Meta input from the encryptor 114 and encrypted by the content key data Kc.

[0258] Here, the A/V decompression software Soft is the software used when decompressing the content file CF in the network apparatus 160_1 and the AV apparatuses 160_2 to 160_4 in the user home network 103 and is for example an ATRAC3 type decompression software.

[0259] Further, the secure container generator 118 generates a key file KF storing, as shown in Fig. 4B, the content key data Kc, usage control policy data (UCP) 106, SAM program download containers SDC_1 to SDC_3, and the signature certificate module Mod_1 encrypted by the distribution key data KD_1 to KD_6 of the corresponding period input from the encryptor 116.

[0260] Then, the secure container generator 118 generates a secure container 104 storing the content file CF and the key file KF shown in Figs. 4A and 4B and the public key data K_{CP} and the signature data $SIG_{1,ESC}$ of the content provider 101 shown in Fig. 4C, stores this in a secure container database 118a, and then outputs the same to the SAM manager 124 in response to a request from the user.

[0261] In this way, in the present embodiment, an in-band method storing the public key certificate CER_{CP} of the public key data $K_{CP,P}$ of the content provider 101 in a secure container 104 and transmitting it to the user home network 103 is employed. Accordingly, it is not necessary for the user home network 103 to communicate with the EMD service center 102 for obtaining the public key certificate CER_{CP}.

[0262] Note that, in the present invention, it is also possible to employ an out-of-band method where the user home network 103 obtains the public key certificate CER_{CP} from the EMD service center 102 without storing

the public key certificate CER_{CP} in the secure container 104.

[0263] The mutual authenticator 120 generates session key data (common key) K_{SES} by mutual authentication between the EMD service center 102 and the user home network 103 when the content provider 101 transfer data on-line between the EMD service center 102 and the user home network 103. The session key data K_{SES} is newly generated at each mutual authentication.

[0264] The encryptor/decryptor 121 encrypts the data to be transmitted by the content provider 101 to the EMD service center 102 and the user home network 103 on-line by using the session key data K_{SES}.

[0265] Further, the encryptor/decryptor 121 decrypts the data received by the content provider 101 from the EMD service center 102 and the user home network 103 on-line by using the session key data K_{SES}.

[0266] The usage control policy data generator 122 generates the usage control policy data 106 and outputs this to the encryptor 116.

[0267] The usage control policy data 106 is a descriptor defining the operation rules of the content data C and describes for example the suggested retailer's price SRP intended by the operator of the content provider 101 and the copying rules of the content data C therein.

[0268] The SAM manager 124 supplies the secure container 104 to the user home network 103 off-line and/or on-line.

[0269] The SAM manager 124 encrypts the secure container 104 by using the distribution key data KD_1 to KD_6 etc. and stores the same on a storage medium when distributing the secure container 104 to the user home network 103 off-line by using a ROM type storage medium such as a CD-ROM or DVD (digital versatile disc). Then, this storage medium is supplied to the user home network 103 off-line by sale or the like.

[0270] In the present embodiment, the secure container (product capsule) 104 is defined by the application layer in the OSI layer as shown in Fig. 5. Further, capsules corresponding to the presentation layer and the transport layer are separately defined from the secure container 104 as transport protocol for transporting the secure container. Accordingly, the secure container 104 can be defined without depending on the transport protocol. Namely, no matter what the mode, that is, on-line or off-line, of supplying the secure container 104 to the user home network 103, the container can be defined and generated according to a common rule.

[0271] For example, when supplying the secure container 104 by using the network, the secure container 104 is defined in a region of the content provider 101, and the presentation layer and the transport layer are considered as transport tools for transporting the secure container 104 to the user home network 103.

[0272] Further, in the off-line case, a ROM type storage medium is considered as a transport carrier for transporting the secure container 104 to the user home network 103.

[0273] Figure 6 is a view for explaining a storage medium 130.

[0274] As shown in Fig. 6, each of the ROM type storage media 130 has a ROM region 131, a RAM region 132, and a media SAM 133.

[0275] The ROM region 131 stores the content file CF shown in Fig. 4A.

[0276] Further, the RAM region 132 stores signature data generated by using a MAC (message authentication code) function using as arguments the key file KF and public key certificate data CER_{CP} shown in Fig. 4B and Fig. 4C and storage key data K_{STR} having an inherent value in accordance with the type of the apparatus and data obtained by encrypting the related key file KF and public key certificate data CER_{CP} by using media key data K_{MED} having a value inherent in the storage media.

[0277] Further, the RAM region 132 stores a public key certificate revocation list for specifying the content provider 101 and SAMs 105_1 to 105_5 which became invalid due to for example an illegal action.

[0278] Further, the RAM region 132, as will be mentioned later, stores usage control status (UCS) data 166 generated when the purchase and/or usage mode of the content data C are determined in the SAMs 105_1 to 105_4 of the user home network 103 etc. By this, by the storage of the usage control status data 166 in the RAM region 132, the ROM type storage medium 130 having the purchase and/or usage mode determined therein is obtained.

[0279] The media SAM 133, for example, stores the media ID as the identifier of the ROM type storage medium 130 and the media key data K_{MED}.

[0280] The media SAM 133 has for example a mutual authentication function.

[0281] Further, the SAM manager 124 encrypts the secure container 104 in the encryptor/decryptor 121 by using the session key data K_{SES} and then distributes the same via the network to the user home network 103 when distributing the secure container 104 to the user home network 103 on-line by using a network, digital broadcast, or the like.

[0282] In the present embodiment, as the SAM manager, EMD service center manager, and a content provider manager and a service provider manager mentioned later, use is made of for example a communication gateway having a tamper resistant structure making it difficult to monitor and tamper the internal processing content.

[0283] Here, for the distribution of the content data C from the content provider 101 to the user home network 103, use is made of the secure container 104 of the common mode storing the usage control policy data 106 in both of the case of distribution using a storage medium 130 as mentioned above and the case of distribution on-line by using a network. Accordingly, in the SAMs 105_1 to 105_4 of the user home network 103, in both of the off-

line and on-line cases, right clearing based on the common usage control policy data 106 is possible.

[0284] Further, as mentioned above, in the present embodiment, the in-band method of enclosing the content data C encrypted by the content key data Kc and the content key data Kc for decrypting the related encryption in the secure container 104 is employed. In the in-band method, there is the advantage that it is not necessary to separately distribute the content key data Kc and the load of network communication can be reduced when it is desired to reproduce the content data C at an apparatus of the user home network 103. Further, the content key data Kc is encrypted by the distribution key data KD_1 to KD_6, but the distribution use public key data KD_1 to KD_6 are managed by the EMD service center 102 and have been distributed to the SAMs 105_1 to 1055 of the user home network 103 in advance (when the SAMs 105_1 to 105_4 access to the EMD service center 102 the first time), therefore, in the user home network 103, the usage of the content data C off-line becomes possible without connecting with the EMD service center 102 on-line.

[0285] Note that, the present invention has the flexibility of enabling use of the out-of-band method of separately supplying the content data C and the content key data Kc to the user home network 103.

[0286] When receiving six months' worth of the distribution key data KD_1 to KD_6 and the corresponding signature data $SIG_{KD1,ESC}$ to $SIG_{KD6,ESC}$, the public key certificate CER_{CP} containing the public key data $K_{CP,P}$ of the content provider 101 and the signature data $SIG_{1,ESC}$ thereof, and the settlement report data 107 from the EMD service center 102, the EMD service center manager 125 decrypts them in the encryptor/decryptor 121 by using the session key data K_{SES}, and then stores them in the storage unit 119.

[0287] The settlement report data 107 describes, for example, the content of the settlement concerning the content provider 101 performed with respect to the settlement organization 91 shown in Fig. 1 by the EMD service center 102.

[0288] Further, the EMD service center manager 125 transmits a global unique identifier Content_ID of the content data C to be provided, the public key data $K_{CP,P}$, and their signature data $SIG_{8,CP}$ to the EMD service center 102 and receives as its input public key certificate data CER_{CP} of public key data $K_{CP,P}$ from the EMD service center 102.

[0289] Further, the EMD service center manager 125 generates a module Mod_3 storing the global unique identifier Content_ID of the content data C to be provided, the content key data Kc, and the usage control policy data 106 therein and a usage control policy registration request use module Mod_2 storing signature data $SIG_{5,CP}$ thereof as shown in Fig. 7A when registering the usage control policy data 106 in the EMD service center 102, encrypts them in the encryptor/decryptor 121 by using the session key data K_{SES}, and then transmits the same via the network to the EMD service center 102. As the EMD service center manager 125, as mentioned before, use is made of for example a communication gateway having the tamper resistant structure making it difficult to monitor and tamper with the internal processing content.

[0290] Below, an explanation will be made of the flow of the processing in the content provider 101 by referring to Fig. 2 and Fig. 3.

[0291] Note that, as a prerequisite of the following processing, a related party of the content provider 101 performs processing for registration at the EMD service center 102 off-line by using for example its own ID card and bank account for the settlement processing and obtains a global unique identifier CP_ID. The global unique identifier CP_ID is stored in the storage unit 119.

[0292] Below, an explanation will be made of the processing when the content provider 101 requests public key certificate data CER_{CP} for certifying the legitimacy of the public key data $K_{CP,S}$ corresponding to its own secret key data $K_{CP,S}$ to the EMD service center 102 by referring to Fig. 3 and Fig. 8.

[0293] Figure 8 is a flowchart of the related processing.

[0294] Step SA1: The content provider 101 generates a random number by using a random number generator 115 configured by for example a true random number generator and generates the secret key data $K_{CP,S}$.

[0295] Step SA2: The content provider 101 generates public key data $K_{CP,P}$ corresponding to the secret key data $K_{CP,S}$ and stores the same in the storage unit 119.

[0296] Step SA3: The EMD service center manager 125 of the content provider 101 reads the identifier CP_ID of the content provider 101 and the public key data $K_{CP,P}$ from the storage unit 119.

[0297] Then, the EMD service center manager 125 transmits a public key certificate data issuance request containing the identifier CP_ID and the public key data $K_{CP,P}$ to the EMD service center 102.

[0298] Step SA4: The EMD service center manager 125 receives as its inputs the public key certificate data CER_{CP} and signature data $SIG_{1,ESC}$ thereof from the EMD service center 102 in response to the related issuance request and writes the same into the storage unit 119.

[0299] Below, an explanation will be made of the processing for receiving the distribution key data from the EMD service center 102 by the content provider 101 by referring to Fig. 3.

[0300] Note that, as the prerequisite for the following processing, the content provider 101 must have already obtained the public key certificate data CER_{CP} from the EMD service center 102.

[0301] The EMD service center manager 125 receives as its inputs six months' worth of the distribution key data KD_1 to KD_3 and their signature data $SIG_{KD1,ESC}$ to $SIG_{KD6,ESC}$ thereof from the EMD service center 102 and stores them in a predetermined data-

base in the storage unit 119.

[0302] Then, in the signature processor 117, after the legitimacy of the signature data $SIG_{KD1,ESC}$ to $SIG_{KD6,ESC}$ stored in the storage unit 119 is confirmed, the distribution key data KD_1 to KD_6 stored in the storage unit 119 are handled as valid data.

[0303] Below, an explanation will be made of the processing when the content provider 101 transmits the secure container 104 to the SAM 105_1 of the user home network 103 referring to Fig. 2 and Fig. 9.

[0304] Figure 9 is a flowchart of the related processing.

[0305] Note that, in the following example, the case of transmitting the secure container 104 from the content provider 101 to the SAM 105_1 is illustrated, but the same applies also to the case of transmitting the secure container 104 to the SAMs 105_2 to 105_4 except it is transmitted to the SAMs 105_2 to 105_4 via the SAM 105_1.

[0306] Step SB1: Content data S111 is read from the content master source server 111 and output to the electronic watermark information adder 112.

[0307] The electronic watermark information adder 112 buries the electronic watermark information in the content data S111 to generate content data S112 and outputs this to the compressor 113.

[0308] Step SB2: The compressor 113 compresses the content data S112 by for example the ATRAC3 method to generate content data S113 and outputs this to the encryptor 114.

[0309] Step SB3: The random number generator 115 generates a random number to generate the content key data Kc and outputs this to the encryptor 114.

[0310] Step SB4: The encryptor 114 encrypts the content data S113 and the meta-data Meta and A/V decompression software Soft read from the storage unit 119 by using the content key data Kc and outputs the same to the secure container generator 118. In this case, the meta-data Meta does not have to be encrypted.

[0311] Then, the secure container generator 118 generates the content file CF shown in Fig. 4A. Also, in the signature processor 117, the hush value of the content file CF is taken, and the signature data $SIG_{8,CP}$ is generated by using the secret key data $K_{CP,S}$.

[0312] Step SB5: The signature processor 117 takes the hush value with respect to each of the content data C, content key data Kc, and the usage control policy data 106 and generates the signature data $SIG_{2,CP}$, $SIG_{3,CP}$, and $SIG_{4,CP}$ indicating the legitimacy of the creator (provider) of the data by using the secret key data $K_{CP,S}$.

[0313] Further, the encryptor 116 encrypts the content key data Kc, usage control policy data 106, SAM program download containers SD_1 to SD_3, and signature certificate module Mod_1 shown in Fig. 4B by the distribution key data KD_1 to KD_3 of the corresponding period and outputs the same to the secure container generator 118.

[0314] Then, the secure container generator 118 generates the key file KF shown in Fig. 4B.

[0315] Further, the signature processor 117 takes the hush value of the key file KF and generates the signature data $SIG_{7,CP}$ by using the secret key data $K_{CP,S}$.

[0316] Step SB6: The secure container generator 118 generates the secure container 104 storing the content file CF and the signature data $SIG_{8,CP}$ thereof shown in Fig. 4A, the key file KF and the signature data $SIG_{7,CP}$ thereof shown in Fig. 4B, and the public key certificate data CER_{CP} and the signature data $SIG_{1,ESC}$ thereof shown in Fig. 4C therein and stores this in the secure container database 118a.

[0317] Step SB7: The secure container generator 118 reads the secure container 104 to be provided to the user home network 103 in response to for example a request from the user from the secure container database 118a, encrypts the same in the encryptor/decryptor 121 by using the session key data K_{SES} obtained by the mutual authentication between the mutual authenticator 120 and the SAM 105_1, and then transmits the same to the SAM 105_1 of the user home network 103 via the SAM manager 124.

[0318] Below, an explanation will be made of the processing in the case where the content provider 101 requests to the EMD service center 102 to register and authorize the usage control policy data 106 and the content key data Kc by referring to Fig. 3.

[0319] The processing for requesting authorization of the usage control policy data 106 and the content key data Kc is carried out for every content data C.

[0320] In this case, the signature processor 117 finds the hush value of the module Mod_3 comprised by the global unique identifier Content_ID of the content data C and the content key data Kc read from the storage unit 119 and the usage control policy data 106 input from the usage control policy data generator 122 and generates the signature data $SIG_{5,CP}$ by using the secret key data $K_{CP,S}$.

[0321] Then, it encrypts the right registration request use module Mod_2 shown in Fig. 7A in the encryptor/decryptor 121 by using the session key data K_{SES} obtained by the mutual authentication between the mutual authenticator 120 and the EMD service center 102, then transmits it from the EMD service center manager 125 to the EMD service center 102.

[0322] In the present embodiment, the case where the content provider 101 does not receive the authorization certificate module certifying that the content provider 101 is authorized from the EMD service center 102 after the EMD service center 102 authorizes the usage control policy data 106 and the content key data Kc, that is, the case where the encryption is carried out in the content provider 101 by using the distribution key data KD_1 to KD_6 to generate the key file KF, is illustrated.

[0323] Note that in the present invention, it is also possible to transmit an authorization certificate module Mod_{2a} shown in Fig. 7B encrypted by using the distribution key data KD_1 to KD_6 from the EMD service center

102 to the content provider 101 after authorization of the usage control policy data 106 and the content key data Kc in the EMD service center 102.

[0324] The authorization certificate module Mod_{2a} stores a module Mod_{3a} storing the global unique identifier Content_ID of the content data C, content key data Kc, and the usage control policy data 106 input from the usage control policy data generator 122 and signature data $SIG_{5a,ESC}$ of the module Mod_{3a} using the secret key data $K_{ESC,S}$.

[0325] In this case, the content provider 101 stores the authorization certificate module Mod_{2a} in for example the secure container 104 and distributes the same to the SAMs 105_1 to 105_4.

[0326] Note that, it is also possible that the EMD service center 102 generate six months' worth of the authorization certificate module Mod_{2a} encrypted by using the distribution key data KD_1 to KD_6 corresponding to different months and transmit them to the content provider 101 together.

[EMD Service Center 102]

[0327] The EMD service center 102 has a certificate authority (CA) function, a key management function, and a right clearing (profit distribution) function.

[0328] Figure 10 is a view of the configuration of the functions of the EMD service center 102.

[0329] As shown in Fig. 10, the EMD service center 102 has a key server 141, a key database 141a, a settlement processor 142, a signature processor 143, a settlement organization manager 144, a certificate/usage control policy manager 145, a CER database 145a, a content provider manager 148, a CP database 148a, a SAM manager 149, a SAM database 149a, a mutual authenticator 150, and an encryptor/decryptor 151.

[0330] Note that, in Fig. 10, in the flow of the data among the functional blocks in the EMD service center 102, the flow of the data related to the data transferred with the content provider 101 is shown.

[0331] Further, in Fig. 11, in the flow of the data among the functional blocks in the EMD service center 102, the flow of the data related to the data transferred between the SAMs 105_1 to 105_4 and the settlement organization 91 shown in Fig. 1 is shown.

[0332] The key server 141 reads the distribution key data having the term of validity of one month stored in the key database 141a in response to a request and outputs the same to the content provider manager 148 and the SAM manager 149.

[0333] Further, it is comprised by a series of the key databases for storing the key data such as the storage key data K_{STR}, media key data K_{MED}, and MAC key data K_{MAC} other than the key database 141a distribution key data KD.

[0334] The settlement processor 142 performs the settlement processing based on the usage log data 108 input from the SAMs 105_1 to 105_4, suggested retailer' price data SRP input from the certificate/usage control policy manager 145, and the sale price, generates the settlement report data 107 and a settlement claim data 152, outputs the settlement report data 107 to the content provider manager 148, and outputs the settlement claim data 152 to the settlement organization manager 144.

[0335] Note that, the settlement processor 142 monitors whether or not the transaction was conducted by an illegal dumping price based on the sale price.

[0336] Here, the usage log data 108 indicates the log of the purchase and the usage (reproduction, storing, transfer, etc.) of the secure container 104 in the user home network 103 and is used when determining the payment of the license fee stored to the secure container 104 in the settlement processor 142.

[0337] The usage log data 108 describes, for example, the identifier Content_ID of the content data C stored in the secure container 104, the identifier CP_ID of the content provider 101 distributing the secure container 104, the compression method of the content data C in the secure container 104, the identifier Media_ID of the storage medium storing the secure container 104, the identifier SAM_ID of the SAMs 105_1 to 105_4 receiving the distribution of the secure container 104, the USER_ID of the related SAMs 105_1 to 105_4, etc. Accordingly, when the EMD service center 102 must distribute money paid by the user of the user home network 103 to a party other than the owner of the content provider 101, for example, the license owner of for example the compression method or the storage medium, the EMD service center 102 determines the sum to be paid to each other party based on a distribution rate table determined in advance and generates the settlement report data 107 and the settlement claim data 152 in accordance with the related determination. The related distribution rate table is generated for example for every content data stored in the secure container 104.

[0338] Further, the settlement claim data 152 is authorized data enabling claim of payment of money to the settlement organization 91 and is generated for each individual owner of a right when for example the money paid by the user is distributed to a plurality of owners of rights.

[0339] Note that the settlement organization 91 sends a record of use of the related settlement organization to the EMD service center 102 when the settlement is finished. The EMD service center 102 notifies the content of the related record of use to the corresponding owner of a right.

[0340] The settlement organization manager 144 transmits the settlement claim data 152 generated by the settlement processor 142 via the payment gateway 90 shown in Fig. 1 to the settlement organization 91.

[0341] Note that, as will be mentioned later, it is also possible that the settlement organization manager 144 transmit the settlement claim data 152 to an owner of a right such as the content provider 101 and that the own-

er of the right itself performs the settlement at the settlement organization 91 by using the received settlement claim data 152.

[0342] Further, the settlement organization manager 144 takes the hush value of the settlement claim data 152 in the signature processor 143 and transmits signature data SIG_{88} generated by using the secret key data $K_{ESC,S}$ together with the settlement claim data 152 to the settlement organization 91.

[0343] The certificate/usage control policy manager 145 reads the public key certificate data CER_{CP} and public key certificate data CER_{SAM1} to CER_{SAM4} etc. registered and authorized in the CER database 145a and, at the same time, registers and authorizes the usage control policy data 106 and the content key data Kc etc. of the content provider 101 in the CER database 145a.

[0344] Note that, it is also possible that databases for storing the public key certificate data CER_{SAM1} to CER_{SAM4}, the usage control policy data 106, and the content key data Kc be individually provided.

[0345] At this time, the certificate/usage control policy manager 145 takes the hush value of for example the usage control policy data 106 and the content key data Kc and generates the authorized public key certificate data having the signature data using the secret key data $K_{ESC,S}$ attached thereto.

[0346] The content provider manager 148 has the function of communicating with the content provider 101 and can access the CP database 148a for managing the identifier CP_ID etc. of the registered content provider 101.

[0347] The SAM manager 149 has the function of communicating with the SAMs 105_1 to 105_4 in the user home network 103 and can access the SAM database 149a storing the identifier SAM_ID of the registered SAM and the SAM registration list etc.

[0348] Below, the flow of the processing in the EMD service center 102 will be explained.

[0349] First, the flow of the processing when transmitting the distribution key data from the EMD service center 102 to the content provider 101 and the SAMs 105_1 to 105_4 in the user home network 103 will be explained while referring to Fig. 10 and Fig. 11.

[0350] As shown in Fig. 10, the key server 141 reads for example six months' worth of the distribution key data KD_1 to KD_6 from the key database 141a every predetermined period and outputs the same to the content provider manager 148.

[0351] Further, the signature processor 143 takes the hush value of each of the distribution key data KD_1 to KD_6, generates the signature data $SIG_{KD1,ESC}$ to $SIG_{KD6,ESC}$ corresponding to them, and outputs them to the content provider manager 148.

[0352] The content provider manager 148 encrypts these six months' worth of the distribution key data KD_1 to KD_6 and their signature data $SIG_{KD1,ESC}$ to $SIG_{KD6,ESC}$ by using the session key data K_{SES} obtained by the mutual authentication between the mutual authenticator 150 and the mutual authenticator 120 shown in Fig. 3 and then transmits the same to the content provider 101.

[0353] Further, as shown in Fig. 11, the key server 141 reads for example three months' worth of the distribution key data KD_1 to KD_3 from the key database 141a for every predetermined period and outputs the same to the SAM manager 149.

[0354] Further, the signature processor 143 takes the hush value of each of the distribution key data KD_1 to KD_3, generates the signature data $SIG_{KD1,ESC}$ to $SIG_{KD3,ESC}$ corresponding to them by using the secret key data $K_{ESC,S}$ of the EMD service center 102, and outputs them to the SAM manager 149.

[0355] The SAM manager 149 encrypts these three months' worth of the distribution key data KD_1 to KD_3 and their signature data $SIG_{KD1,ESC}$ to $SIG_{KD3,ESC}$ by using the session key data K_{SES} obtained by mutual authentication between the mutual authenticator 150 and the SAMs 105_1 to 105_4 and then transmits the same to the SAMs 105_1 to 105_4.

[0356] Below, an explanation will be made of the processing where the EMD service center 102 receives a request for issuance of public key certificate data CER_{CP} from the content provider 101 by referring to Fig. 10 and Fig. 12.

[0357] Figure 12 is a flowchart of the related processing.

[0358] Step SC1: When receiving a request for issuance of public key certificate data containing the identifier CP_ID of the content provider 101, public key data $K_{CP,P}$, and signature data $SIG_{8,CP}$ from the content provider 101, the content provider manager 148 decrypts them by using the session key data K_{SES} obtained by mutual authentication between the mutual authenticator 150 and the mutual authenticator 120 shown in Fig. 3.

[0359] Step SC2: After confirming the legitimacy of the related decrypted signature data $SIG_{8,CP}$ at the signature processor 143, it confirms whether or not the content provider 101 issuing the related public key certificate data issuance request is registered in the CP database 148a based on the identifier CP_ID and the public key data $K_{CP,P}$.

[0360] Step SC3: The certificate/usage control policy manager 145 reads the public key certificate data CER_{CP} of the related content provider 101 from the CER database 145a and outputs the same to the content provider manager 148.

[0361] Step SC4: The signature processor 143 takes the hush value of the public key certificate data CER_{CP}, generates the signature data $SIG_{1,ESC}$ by using the secret key data $K_{ESC,S}$ of the EMD service center 102, and outputs this to the content provider manager 148.

[0362] Step SC5: The content provider manager 148 encrypts the public key certificate data CER_{CP} and the signature data $SIG_{1,ESC}$ thereof by using the session key data K_{SES} obtained by the mutual authentication be-

tween the mutual authenticator 150 and the mutual authenticator 120 shown in Fig. 3 and then transmits the same to the content provider 101.

[0363] Below, an explanation will be made of the processing where the EMD service center 102 receives a request for issuance of public key certificate data CER_{SAM1} from the SAM 105_1 by referring to Fig. 11 and Fig. 13.

[0364] Figure 13 is a flowchart of the related processing.

[0365] Step SD1: When receiving a request for issuance of public key certificate data containing the identifier SAM1_ID of the SAM 105_1, the public key data $K_{SAM1,P}$, and the signature data $SIG_{8,SAM1}$ from the SAM 105_1, the SAM manager 149 decrypts them by using the session key data K_{SES} obtained by the mutual authentication between the mutual authenticator 150 and the SAM 105_1.

[0366] Step SD2: After confirming the legitimacy of the related decrypted signature data $SIG_{8,SAM1}$ at the signature processor 143, it is confirmed whether or not the SAM 105_1 issuing a request for issuance of the related public key certificate data is registered in the SAM database 149a based on the identifier SAM1_ID and the public key data $K_{SAM1,P}$.

[0367] Step SD3: The certificate/usage control policy manager 145 reads the public key certificate data CER_{SAM1} of the related SAM 105_1 from the CER database 145a and outputs the same to the SAM manager 149.

[0368] Step SD4: The signature processor 143 takes the hush value of the public key certificate data CER_{SAM1}, generates signature data $SIG_{50,ESC}$ by using the secret key data $K_{ESC,S}$ of the EMD service center 102, and outputs this to the SAM manager 149.

[0369] Step SD5: The SAM manager 149 encrypts the public key certificate data CER_{SAM1} and the signature data $SIG_{50,ESC}$ thereof by using the session key data K_{SES} obtained by the mutual authentication between the mutual authenticator 150 and the SAM 105_1 and then transmits the same to the SAM 105_1.

[0370] Note that the processing where the SAMs 105_2 to 105_4 request public key certificate data is basically the same as the case of the SAM 105_1 mentioned above except the object is replaced by the SAMs 105_2 to 105_4.

[0371] Note that, in the present invention, the EMD service center 102 can generate the public key certificate data CER_{SAM1} of the public key data $K_{SAM1,P}$ too at the time of shipping when for example storing the secret key data $K_{SAM1,S}$ and the public key data $K_{SAM1,P}$ of the SAM 105_1 in the storage unit of the SAM 105_1 at the time of shipping of the SAM 105_1.

[0372] At this time, it is also possible to store public key certificate data CER_{SAM1} in the storage unit of the SAM 105_1 at the time of shipping.

[0373] Below, an explanation will be made of the processing where the EMD service center 102 receives a request for registration of the usage control policy data 106 and the content key data Kc from the content provider 101 by referring to Fig. 10 and Fig. 14.

[0374] Figure 14 is a flowchart of the related processing.

[0375] Step SE1: When receiving the usage control policy registration request module Mod_2 shown in Fig. 7A from the content provider 101, the content provider manager 148 decrypts the usage control policy registration request module Mod_2 by using the session key data K_{SES} obtained by the mutual authentication between the mutual authenticator 150 and the mutual authenticator 120 shown in Fig. 3.

[0376] Step SE2: The signature processor 143 verifies the legitimacy of the signature data $SIG_{5,CP}$ by using the public key data K_{CP} read from the key database 141a.

[0377] Step SE3: The certificate/usage control policy manager 145 registers the usage control policy data 106 and the content key data Kc stored in the usage control policy registration request module Mod_2 in the CER database 145a.

[0378] Below, an explanation will be made of the processing where the settlement processing is carried out in the EMD service center 102 by referring to Fig. 11 and Fig. 15.

[0379] Figure 15 is a flowchart of the related processing.

[0380] Step SF1: When receiving as its input the user log data 108 and a signature data $SIG_{200,SAM1}$ thereof from for example the SAM 105_1 of the user home network 103, the SAM manager 149 decrypts the usage log data 108 and the signature data $SIG_{200,SAM1}$ by using the session key data K_{SES} obtained by the mutual authentication between the mutual authenticator 150 and the SAM 105_1, verifies the signature data $SIG_{200,SAM1}$ by the public key data K_{SAM1} of the SAM 105_1, and then outputs the same to the settlement processor 142.

[0381] Step SF2: The settlement processor 142 performs the settlement processing based on the usage log data 108 input from the SAM manager 149 and the suggested retailer' price data SRP and the sale price contained in the usage control policy data 106 read from the CER database 145a via the certificate/usage control policy manager 145 and generates the settlement claim data 152 and the settlement report data 107. Note that, the settlement claim data 152 and the settlement report data 107 can be generated whenever the usage log data 108 is input from the SAM too or can be generated for every predetermined period too.

[0382] Step SF3: The settlement processor 142 outputs the settlement claim data 152 to the settlement organization manager 144.

[0383] The settlement organization manager 144 transmits the settlement claim data 152 and the signature data SIG_{88} thereof via the payment gateway 90 shown in Fig. 1 to the settlement organization 91 after the mutual authentication and the decryption by the session key data K_{SES}.

[0384] By this, money of the sum indicated in the settlement claim data 152 is paid to the content provider 101.

[0385] Note that, it is also possible for the EMD service center 102 to transmit the settlement claim data 152 to the content provider 101 and for the content provider 101 to claim money at the settlement organization 91 by using the settlement claim data 152.

[0386] Step SF4: The settlement processor 142 outputs the settlement report data 107 to the content provider manager 148.

[0387] The settlement report data 107, as mentioned above, describes for example the content of the settlement concerning the content provider 101 performed with respect to the settlement organization 91 shown in Fig. 1 by the EMD service center 102.

[0388] The content provider manager 148 encrypts the settlement report data 107 by using the session key data K_{SES} obtained by the mutual authentication between the mutual authenticator 150 and the mutual authenticator 120 shown in Fig. 3 and then transmits the same to the content provider 101.

[0389] Further, it is also possible that the EMD service center 102 register (authorize) the usage control policy data 106 as mentioned above and then encrypt the authorization certificate module Mod_{2a} shown in Fig. 7B by the distribution key data KD_1 to KD_6 and transmit the same from the EMD service center 102 to the content provider 101.

[0390] Further, the EMD service center 102 performs the processing at the time of shipment of the SAMs 105_1 to 105_4 and the registration processing of the SAM registration list other than the above. These processings will be explained later.

[User Home Network 103]

[0391] The user home network 103 has the network apparatus 160_1 and the A/V apparatuses 160_2 to 160_4 as shown in Fig. 1.

[0392] The network apparatus 160_1 includes the SAM 105_1. Further, the AV apparatuses 160_2 to 160_4 include the SAMs 105_2 to 105_4.

[0393] The SAMs 105_1 to 105_4 are connected to each other via the bus 191, for example, the IEEE 1394 serial interface bus.

[0394] Note that, it is also possible that the AV apparatuses 160_2 to 160_4 have the network communication function or do not have the network communication function, but utilize the network communication function of the network apparatus 160_1.

[0395] Further, it is also possible for the user home network 103 to have only the AP apparatus not having a network function.

[0396] Below, an explanation will be made of the network apparatus 160_1.

[0397] Figure 16 is a view of the configuration of the network apparatus 160_1.

[0398] As shown in Fig. 16, the network apparatus 160_1 has the SAM 105_1, a communication module 162, a decryption/decompression module 163, a purchase/usage mode determination controller 165, a download memory 167, a reproduction module 169, and an external memory 201.

[0399] The SAMs 105_1 to 105_4 are modules for the charge processing in units of content and communicate with the EMD service center 102.

[0400] The SAMs 105_1 to 105_4, for example, are managed in specifications and versions by the EMD service center 102 and are licensed to manufactures of home apparatuses as black box charging modules for charging in units of content when desired to be mounted. For example, a manufacturer developing a home apparatus cannot learn the internal specifications of the ICs (integrated circuit) of the SAMs 105_1 to 105_4. The EMD service center 102 standardizes the interfaces etc. of the related ICs. These are mounted in the network apparatus 160_1 and the AV apparatuses 160_2 to 160_4 accordingly.

[0401] The SAMs 105_1 to 105_4 are hardware modules (IC modules etc.) with processing contents completely shut off from the outside and thereby having tamper resistance preventing the processing contents from being monitored or tampered with from the outside and preventing data stored in the inside in advance and the data being processed from being monitored and tampered from the outside.

[0402] When realizing the functions of the SAM 105_1 to 105_4 in the form of ICs, the ICs have secret memories and store secret programs and secret data therein. The SAMs are not limited to the physical mode of ICs. If the functions can be built into a portion of the apparatus, it is also possible to define that portion as a SAM.

[0403] Below, the functions of the SAM 105_1 will be explained in detail.

[0404] Note that, the SAMs 105_2 to 105_4 basically have the same functions as those of the SAM 105_1.

[0405] Figure 17 is a view of the configuration of the functions of the SAM 105_1.

[0406] Note that, in Fig. 17, the flow of the data related to the processing for inputting the secure container 104 from the content provider 101 and decrypting the key file KF in the secure container 104 is shown.

[0407] As shown in Fig. 17, the SAM 105_1 has a mutual authenticator 170, encryptor/decryptors 171, 172, and 173, a content provider manager 180, an error corrector 181, a download memory manager 182, a secure container decryptor 183, a decryption/decompression module manager 184, an EMD service center manager 185, a usage monitor 186, a charge processor 187, a signature processor 189, a SAM manager 190, a media SAM manager 197, a stack (work) memory 200, and an external memory manager 811.

[0408] Note that the AV apparatuses 160_2 to 160_4 do not have download memories 167, therefore there are no download memory managers 182 in the SAMs 105_2 to 105_4.

[0409] Note that, the predetermined functions of the SAM 105_1 shown in Fig. 17 are realized by executing a secret program in for example a not illustrated CPU.

[0410] Further, the stack memory 200 stores the usage log data 108 and the SAM registration list after the following processings as shown in Fig. 18.

[0411] Here, the memory space of the external memory 201 cannot be seen from the outside (for example a host CPU 810) of the SAM 105_1. Only the SAM 105_1 can manage the access with respect to the storage region of an external memory 201.

[0412] As the external memory 201, use is made of for example a flash memory or a ferroelectric memory (FeRAM).

[0413] Further, as the stack memory 200, use is made of for example a SARAM. As shown in Fig. 19, the secure container 104, content key data Kc, usage control policy data (UCP) 106, a lock key data K_{LOC} of a storage unit 192, the public key certificate CER_{CP} of the content provider 101, the usage control status data (UCS) 166, the SAM program download containers SDC_1 to SDC_3, etc. are stored.

[0414] Below, an explanation will be made of the processing content of the functional blocks when inputting the secure container 104 from the content provider 101 among the functions of the SAM 105_1 by referring to Fig. 17.

[0415] When the SAM 105_1 transfers data on-line with the content provider 101 and the EMD service center 102, the mutual authenticator 170 performs the mutual authentication between the content provider 101 and the EMD service center 102 to generate the session key data (common key) K_{SES} and outputs this to the encryptor/decryptor 171. The session key data K_{SES} is newly generated whenever mutual authentication is carried out.

[0416] The encryptor/decryptor 171 encrypts and/or decrypts the data transferred with the content provider 101 and the EMD service center 102 by using the session key data K_{SES} generated by the mutual authenticator 170.

[0417] The error corrector 181 corrects the error of the secure container 104 and outputs the result to the download memory manager 182.

[0418] Note that, it is also possible that the user home network 103 have the function of detecting whether or not the secure container 104 has been tampered with.

[0419] In the present embodiment, the case where the error corrector 181 was included in the SAM 105_1 was illustrated, but it is also possible to impart the function of the error corrector 181 to the outside of the SAM 105_1, for example the host CPU 810.

[0420] The download memory manager 182 encrypts the secure container 104 after the error correction by using the session contained K_{SES} obtained by the mutual authentication after the mutual authentication between the mutual authenticator 170 and a media SAM 167a when the download memory 167 has the media SAM 167a having the mutual authentication function as shown in Fig. 16 and writes the same into the download memory 167 shown in Fig. 16. As the download memory 167, use is made of a nonvolatile semiconductor memory, for example, a memory stick.

[0421] Note that, as shown in Fig. 20, when a memory not provided with a mutual authentication function such as an HDD (hard disk drive) is used as a download memory 211, the interior of the download memory 211 is not secure, therefore the content file CF is downloaded in the download memory 211, and the key file KF having the high secrecy is downloaded in the stack memory 200 shown in Fig. 17.

[0422] The secure container decryptor 183 decrypts the key file KF stored in the secure container 104 input from the download memory manager 182 by using the distribution key data KD_1 to KD_3 of the corresponding period read from the storage unit 192 and confirms the legitimacy of the signature data $SIG_{2,CP}$ to $SIG_{4,CP}$, that is, the legitimacy of the creator of the content data C, content key data Kc, and the usage control policy data 106 in the signature processor 189, and then writes the decrypted data into the stack memory 200.

[0423] The EMD service center manager 185 manages the communication with the EMD service center 102 shown in Fig. 1.

[0424] The signature processor 189 verifies the signature data in the secure container 104 by using the public key data $K_{ESC,P}$ of the EMD service center 102 read from the storage unit 192 and the public key data $K_{CP,P}$ of the content provider 101.

[0425] The storage unit 192 stores, as secret data which cannot be read and rewritten from the outside of the SAM 105_1, as shown in Fig. 21, the distribution key data KD_1 to KD_3, SAM_ID, user ID, password, information reference use ID, SAM registration list, storage key data K_{STR}, public key data $K_{R\text{-}CA,P}$ of the route CA, public key data $K_{ESC,P}$ of the EMD service center 102, media key data K_{MED}, public key data $K_{ESC,P}$ of the EMD service center 102, secret key data $K_{SAM1,S}$ of the SAM 105_1, public key certificate data CER_{SAM1} storing public key data $K_{SAM1,P}$ of the SAM 105_1 therein, signature data SIG_{22} of the public key certificate CER_{ESC} using the secret key data $K_{ESC,S}$ of the EMD service center 102, the original key data for the mutual authentication with the decryption/decompression module 163, and the original key data for the mutual authentication with the media SAM.

[0426] Further, the storage unit 192 stores a secret program for realizing at least part of the functions shown in Fig. 17.

[0427] As the storage unit 192, use is made of for example a flash-EEPROM (electrically erasable programmable RAM).

[0428] Below, an explanation will be made of the flow of the processing when inputting the secure container 104 from the content provider 101 in the flow of the processing of the SAM 105_1.

[0429] First, the flow of the processing in the SAM 105_1 when storing the distribution key data KD_1 to KD_3 received from the EMD service center 102 in the storage unit 192 will be explained by referring to Fig. 17.

[0430] In this case, first, the mutual authentication is carried out between the mutual authenticator 170 and the mutual authenticator 150 shown in Fig. 10.

[0431] Next, three months' worth of the distribution key data KD_1 to KD_3 encrypted by the session key data K_{SES} obtained by the related mutual authentication and the signature data $SIG_{KD1,ESC}$ to $SIG_{KD3,ESC}$ thereof are written from the EMD service center 102 via the EMD service center manager 185 into the stack memory 811.

[0432] Next, the encryptor/decryptor 171 uses the session key data K_{SES} to decrypt the distribution key data KD_1 to KD_3 and the signature data $SIG_{KD1,ESC}$ to $SIG_{KD3,ESC}$.

[0433] Next, the signature processor 189 confirms the legitimacy of the signature data $SIG_{KD1,ESC}$ to $SIG_{KD3,ESC}$ stored in the stack memory 811, then writes the distribution key data KD_1 to KD_3 into the storage unit 192.

[0434] Below, an explanation will be made of the flow of the processing in the SAM 105_1 when inputting the secure container 104 from the content provider 101 and decrypting the key file KF in the secure container 104 by referring to Fig. 17 and Fig. 22.

[0435] Figure 22 is a flowchart of the related processing.

[0436] Step SG1: The mutual authentication is carried out between the mutual authenticator 170 of the SAM 105_1 shown in Fig. 17 and the mutual authenticator 120 shown in Fig. 2.

[0437] The encryptor/decryptor 171 decrypts the secure container 104 received from the content provider 101 via the content provider manager 180 by using the session key data K_{SES} obtained by the related mutual authentication.

[0438] Step SG2: The signature processor 189 verifies the signature data $SIG_{1,ESC}$ shown in Fig. 4C and then confirms the legitimacy of the signature data $SIG_{8,CP}$ and $SIG_{7,CP}$ by using the public key data $K_{CP,P}$ of the content provider 101 stored in the public key certificate data CER_{CP} shown in Fig. 4C.

[0439] When the legitimacy of the signature data $SIG_{8,CP}$ and $SIG_{7,CP}$ is confirmed, the content provider manager 180 outputs the secure container 104 to the error corrector 181.

[0440] The error corrector 181 corrects the error of the secure container 104 and then outputs the result to the download memory manager 182.

[0441] Step SG3: The download memory manager 182 performs the mutual authentication between the mutual authenticator 170 and the media SAM 167a shown in Fig. 16 and then writes the secure container 104 into the download memory 167.

[0442] Step SG4: The download memory manager 182 performs the mutual authentication between the mutual authenticator 170 and the media SAM 167a shown in Fig. 16 and then reads the key file KF shown in Fig. 4B stored in the secure container 104 from the download memory 167 and outputs the same to the secure container decryptor 183.

[0443] Then, the secure container decryptor 183 decrypts the key file KF by using the distribution key data KD_1 to KD_3 of the corresponding period input from the storage unit 192 and outputs the signature data $SIG_{1,ESC}$ and $SIG_{2,CP}$ to $SIG_{4,CP}$ stored in the signature/certificate module Mod_1 shown in Fig. 4B to the signature processor 189.

[0444] Step SG5: The signature processor 189 verifies the signature data $SIG_{1,ESC}$ shown in Fig. 4B and then verifies the signature data $SIG_{2,CP}$ to $SIG_{4,CP}$ by using the public key data $K_{ESC,P}$ stored in the public key certificate data CER_{CP} shown in Fig. 4B. By this, the legitimacy of the creator of the content data C, content key data Kc, and the usage control policy data 106 is verified.

[0445] Step SG6: The secure container decryptor 183 writes the key file KF into the stack memory 200 when the legitimacy of the signature data $SIG_{2,CP}$ to $SIG_{4,CP}$ is confirmed.

[0446] Below, an explanation will be made of the processing content of the functional blocks related to the processing for using and/or purchasing the content data C downloaded in the download memory 167 by referring to Fig. 23.

[0447] The usage monitor 186 reads the usage control policy data 106 and the usage control status data 166 from the stack memory 200 and monitors so that the content is purchased and/or used within the range permitted by the related read usage control policy data 106 and usage control status data 166.

[0448] Here, the usage control policy data 106 has been stored in the key file KF shown in Fig. 4B stored in the stack memory 200 after decryption as explained by using Fig. 17.

[0449] Further, the usage control status data 166 is stored in the stack memory 200 when the purchase mode is determined by the user as will be mentioned later.

[0450] The charge processor 187 generates the usage log data 108 in response to a control signal S165 from the purchase/usage mode determination controller 165 shown in Fig. 16.

[0451] Here, the usage log data 108 describes the log of the purchase and usage modes of the secure container 104 by the user as mentioned before and is used when performing the settlement processing in accordance with the purchase of the secure container 104 and determining the payment of the license fee in the EMD service center 102.

[0452] Further, the charge processor 187 notifies the sale price or the suggested retailer' price data SRP read from the stack memory 200 to the user according to need.

[0453] Here, the sale price and the suggested retailer' price data SRP have been stored in the usage control policy data 106 of the key file KF shown in Fig. 4B stored in the stack memory 200 after decryption.

[0454] The charge processing by the charge processor 187 is carried out based on the content of the rights such as the license conditions indicated by the usage control policy data 106 and the usage control status data 166 under the monitoring of the usage monitor 186. Namely, the user purchases and uses the content within the range according to the related content of rights etc.

[0455] Further, the charge processor 187 generates the usage control status (UCS) data describing the purchase mode of the content by the user and writes this into the stack memory 200.

[0456] As the purchase modes of the content, there are for example a straight purchase without restriction as to reproduction by the purchaser and copying for the usage of the related purchaser and a reproduction charge charging whenever it is reproduced.

[0457] Here, the usage control status data 166 is generated when the user determines the purchase mode of the content, then is used for control so that the user uses the related content within the range permitted by the related determined purchase mode. The usage control status data 166 describes the ID of the content, the purchase mode, the price in accordance with the related purchase mode, the SAM_ID of the SAM with the purchase of the related content performed therefor, USER_ID of the purchasing user, etc.

[0458] Note that, where the determined purchase mode is the reproduction charge, for example, the usage control status data 166 is transmitted from the SAM 105_1 to the content provider 101 in real-time simultaneously with the purchase of the content data C, and the content provider 101 indicates to the EMD service center 102 to obtain the usage log data 108 at the SAM 105_1 within the predetermined period.

[0459] Further, where the determined purchase mode is a straight purchase, for example, the usage control status data 166 is transmitted in real-time to both of the content provider 101 and the EMD service center 102. In this way, in the present embodiment, in the both cases, the usage control status data 166 is transmitted in real-time to the content provider 101.

[0460] The EMD service center manager 185 transmits the usage log data 108 read from the external memory 201 via the external memory manager 811 to the EMD service center 102.

[0461] At this time, the EMD service center manager 185 generates the signature data $SIG_{200,SAM1}$ of the usage log data 108 by using the secret key data $K_{SAM1,S}$ in the signature processor 189 and transmits the signature data $SIG_{200,SAM1}$ together with the usage log data 108 to the EMD service center 102.

[0462] The usage log data 108 can be transmitted to the EMD service center 102 in response to for example a request from the EMD service center 102 or periodically or can be transmitted when the amount of the log information contained in the usage log data 108 becomes the predetermined amount or more. The related amount of information is determined in accordance with for example the storage capacity of the external memory 201.

[0463] The download memory manager 182 outputs the content data C read from the download memory 167, the content key data Kc read from the stack memory 200, and the user watermark data 196 input from the charge processor 187 to the decryption/decompression module manager 184 in the case where for example the reproduction operation of the content is carried out in response to a control signal S165 from the purchase mode determination controller 165 shown in Fig. 16.

[0464] Further, the decryption/decompression module manager 184 outputs the content file CF read from the download memory 167 and the content key data Kc and a semi-disclosure parameter data 199 read from the stack memory 200 to the decryption/decompression module manager 184 when performing a trial listening operation of the content in response to the control signal S165 from the purchase mode determination controller 165 shown in Fig. 16.

[0465] Here, the semi-disclosure parameter data 199 is described in the usage control policy data 106 and indicates the handling of the content in the trial listening mode. In the decryption/deoompression module 163, it becomes possible to reproduce the encrypted content data C in the semi-disclosure state based on the semi-disclosure parameter data 199. As the procedure of the semi-disclosure, there is for example a procedure of designating the blocks to be decrypted and the blocks not to be decrypted by using the content key data Kc, limiting the reproduction function at the time of trial listening, or limiting a trial listening enable period by the semi-disclosure parameter data 199 by utilizing the fact that the decryption/decompression module 163 processes the data (signal) in units of predetermined blocks.

[0466] Below, an explanation will be made of the flow of the processing in the SAM 105_1.

[0467] First, an explanation will be made of the flow of the processing up to when the purchase mode of the secure container 104 downloaded in the download memory 167 from the content provider 101 is determined by referring to Fig. 23 and Fig. 24.

[0468] Figure 24 is a flowchart of the related processing.

[0469] Step SH1: In the charge processor 187, it is decided whether or not the control signal S165 indicating the trial listening mode was generated by the operation of the purchase/usage mode determination controller 165 shown in Fig. 16 by the user. When it is decided that it was generated, the processing of step SH2 is carried out, while when it was not so generated, the processing of step SH3 is carried out.

[0470] Step SH2: By the charge processor 187, for example, the content file CF stored in the download mem-

ory 167 is output via the decryption/decompression module manager 184 to the decryption/decompression module 163 shown in Fig. 16.

[0471] At this time, the mutual authentication between the mutual authenticator 170 and the media SAM 167a and the encryption and/or decryption by the session key data K_{SES} and the mutual authentication between the mutual authenticator 170 and the mutual authenticator 220 and the encryption and/or decryption by the session key data K_{SES} are carried out with respect to the content file CF.

[0472] The content file CF is decrypted at a decryptor 221 shown in Fig. 16 and then output to a decryptor 222.

[0473] Further, the content key data Kc and the semi-disclosure parameter data 199 read from the stack memory 200 are output to the decryption/decompression module 163 shown in Fig. 16. At this time, after the mutual authentication between the mutual authenticator 170 and the mutual authenticator 220, the encryption and decryption by the session key data K_{SES} are carried out with respect to the content key data Kc and the semi-disclosure parameter data 199.

[0474] Next, the decrypted semi-disclosure parameter data 199 is output to a semi-disclosure processor 225, and the content data Cis decrypted using the content key data Kc by the decryptor 222 by semi-disclosure under the control from the semi-disclosure processor 225.

[0475] Next, the content data C decrypted by semi-disclosure is decompressed at a decompression unit 223 and then output to an electronic watermark information processor 224.

[0476] Next, the user watermark data 196 is buried in the content data C in the electronic watermark information processor 224, then the content data C is reproduced at the reproduction module 169, and the audio in accordance with the content data C is output.

[0477] Step SH3: When the user determines the purchase mode by operating the purchase/usage mode determination controller 165, the control signal S165 indicating the related determined purchase mode is output to the charge processor 187.

[0478] Step SH4: In the charge processor 187, the usage log data 108 and the usage control status data 166 in accordance with the determined purchase mode are generated, the usage log data 108 is written into the external memory 201 via the external memory manager 811, and the usage control status data 166 is written into the stack memory 200.

[0479] Thereafter, in the usage monitor 186, control (monitoring) is carried out so that the content are purchased and used within the range permitted by the usage control status data 166.

[0480] Step SH5: The usage control status data 166 is added to the key file KF stored in the stack memory 200 to generate a new key file KF_1 having the purchase mode determined therein shown in Fig. 29B mentioned later. The key file KF_1 is stored in the stack memory 200.

[0481] As shown in Fig. 29B, the usage control status data 166 stored in the key file KF_1 has been encrypted by utilizing the CBC mode of the DES by using the storage key data K_{STR}. Further, the MAC value generated by using the related storage key data K_{STR} as the MAC key data, that is, MAC_{300}, is added. Further, a module comprised by the usage control status data 166 and the MAC_{300} is encrypted by utilizing the CBC mode of the DES by using the media key data K_{MED}. Further, the MAC value generated by using the related media key data K_{MED} as the MAC key data, that is, MAC_{301}, is added to the related module.

[0482] Below, an explanation will be made of the flow of the processing in the case where the content data C having the purchase mode already determined and stored in the download memory 167 is reproduced by referring to Fig. 23 and Fig. 25.

[0483] Figure 25 is a flowchart of the related processing.

[0484] Step SI1: The charge processor 187 receives as its input the control signal S165 designating the content to be reproduced in accordance with the operation by the user.

[0485] Step SI2: In the charge processor 187, the content file CF stored in the download memory 167 is read based on the control signal S165 under the monitoring of the usage monitor 186.

[0486] Step SI3: The related read content file CF is output to the decryption/decompression module 163 shown in Fig. 16. At this time, the mutual authentication is carried out between the mutual authenticator 170 shown in Fig. 23 and the mutual authenticator 220 of the decryption/decompression module 163 shown in Fig. 16.

[0487] Further, the content key data Kc read from the stack memory 200 is output to the decryption/decompression module 163.

[0488] Step SI4: The decryptor 222 of the decryption/decompression module 163 decrypts the content file CF using the content key data Kc and the decompression processing by the decompression unit 223 and reproduces the content data C at the reproduction module 169.

[0489] Step SI5: The charge processor 187 updates the usage log data 108 stored in the external memory 201 in response to the control signal S165.

[0490] The usage log data 108 is read from the external memory 201, and then passes through the mutual authentication and is transmitted via the EMD service center manager 185 together with the signature data SIG200,SAM1 to the EMD service center 102.

[0491] Below, an explanation will be made of the flow of the processing in the SAM 105_1 in a case where, as shown in Fig. 26, for example the content file CF having the purchase mode already determined and downloaded in the download memory 167 of the network apparatus 160_1 and the key file KF are transferred to the SAM 105_2 of the AV apparatus 160_2 via the bus 191 by refer-

ring to Fig. 27 and Fig. 28.

[0492] Figure 28 is a flowchart of the related processing.

[0493] Step SJ1: The user operates the purchase/usage mode determination controller 165 and indicates the transfer of the predetermined content stored in the download memory 167 to the AV apparatus 160_2, and the control signal S165 in accordance with the related operation is output to the charge processor 187.

[0494] By this, the charge processor 187 updates the usage log data 108 stored in the external memory 201 based on the control signal S165.

[0495] Step SJ2: The download memory manager 182 outputs the content file CF shown in Fig. 29A read from the download memory 167 to the SAM manager 190.

[0496] Step SJ3: The key file KF_1 shown in Fig. 29B read from the stack memory 200 is output to the signature processor 189 and the SAM manager 190.

[0497] Step SJ4: The signature processor 189 generates signature data $SIG_{42,SAM1}$ of the key file KF_1 read from the stack memory 200 and outputs this to the SAM manager 190.

[0498] Further, the SAM manager 190 reads public key certificate data CER_{SAM1} shown in Fig. 29C and signature data $SIG_{22,ESC}$ thereof from the storage unit 192.

[0499] Step SJ5: The mutual authenticator 170 outputs the session key data K_{SES} obtained by the mutual authentication with the SAM 105_2 to the encryptor/decryptor 171.

[0500] The SAM manager 190 generates a new secure container comprised by data shown in Fig. 29A, Fig. 29B, and Fig. 29C.

[0501] Step SJ6: The encryptor/decryptor 171 encrypts the data by using the session key data K_{SES} and then output it to the SAM 105_2 of the AV apparatus 1602 shown in Fig. 26.

[0502] At this time, parallel to the mutual authentication between the SAM 105_1 and the SAM 105_2, the mutual authentication of the bus 191 as the IEEE1394 serial bus is carried out.

[0503] Below, as shown in Fig. 26, the flow of the processing in the SAM 105_2 when writing the content file CF etc. input from the SAM 105_1 into a storage media such as a RAM type will be explained by referring to Fig. 30 and Fig. 31.

[0504] Figure 31 is a flowchart of the related processing.

[0505] Step SK1: The SAM manager 190 of the SAM 105_2 receives as its inputs the content file CF shown in Fig. 29A, key file KF_1, and the signature data $SIG_{42,SAM1}$ thereof shown in Fig. 29B and public key certificate data CER_{SAM1} and the signature data $SIG_{22,ESC}$ thereof shown in Fig. 29C from the SAM 105_1 of the network apparatus 160_1 as shown in Fig. 26.

[0506] Then, the encryptor/decryptor 171 decrypts the content file CF, the key file KF_1 and the signature data $SIG_{42,SAM1}$ thereof, and the public key certificate data CER_{SAM1} and the signature data $SIG_{22,ESC}$ thereof input by the SAM manager 190 by using the session key data K_{SES} obtained by the mutual authentication between the mutual authenticator 170 and the mutual authenticator 170 of the SAM 105_1.

[0507] Next, the key file KF_1 and the signature data $SIG_{42,SAM1}$ thereof and public key certificate data CER_{SAM1} and the signature data $SIG_{22,ESC}$ thereof decrypted by using the session key data K_{SES} are written into the stack memory 200.

[0508] Step SK2: The signature processor 189 verifies the signature data $SIG_{22,ESC}$ read from the stack memory 200 by using the public key data $K_{ESC,P}$ read from the storage unit 192 and confirms the legitimacy of public key certificate data CER_{SAM1}.

[0509] Then, the signature processor 189 confirms the legitimacy of the signature data $SIG_{42,SAM1}$ by using the public key data $K_{SAM1,P}$ stored in the public key certificate data CER_{SAM1} when confirming the legitimacy of the public key certificate data CER_{SAM1}.

[0510] Next, when the legitimacy of the signature data $SIG_{42,SAM1}$, that is the legitimacy of the creator of the key file KF_1, is confirmed, it reads the key file KF_1 shown in Fig. 29B from the stack memory 200 and outputs it to the encryptor/decryptor 173.

[0511] Note that, in the related example, the case where the creator of the key file KF_1 and the source of transmission were the same was explained, but when the creator of the key file KF1 and the source of transmission are different, the signature data of the creator and the signature data of the transmitter are generated with respect to the key file KF_1 and the legitimacy of both signature data is verified at the signature processor 189.

[0512] Step SK3: The encryptor/decryptor 173 sequentially encrypts the key file KF_1 by using the storage key data K_{STR}, media key data K_{MED}, and purchaser key data K_{PIN} read from the storage unit 192 and outputs the same to the media SAM manager 197.

[0513] Note that, the media key data K_{MED} is stored in the storage unit 192 in advance by the mutual authentication between the mutual authenticator 170 shown in Fig. 27 and the media SAM 252 of the RAM type storage media 250 shown in Fig. 26.

[0514] Here, the storage key data K_{STR} is the data determined in accordance with the type of the apparatus, for example, a SACD (super audio compact disc) or DVD (digital versatile disc) apparatus, CD-R apparatus, and MD (Mini Disc) apparatus (AV apparatus 160_2 in the related example) and is used for establishing a one-to-one correspondence between the types of the apparatuses and the types of the storage media. Note that the physical configurations of the disc media are the same between an SACD and a DVD, so there is a case where the storage and/or reproduction of the SACD storage media can be carried out by using a DVD apparatus. The storage key data K_{STR} plays te role of preventing illicit copying in such a case.

[0515] Further, the media key data K_{MED} is data

unique to the storage medium (the RAM type storage medium 250 in the related example).

[0516] The media key data K_{MED} is stored in the storage media (the RAM type storage media 250 shown in Fig. 26 in the related example) side and preferably performs the encryption and decryption using the media key data K_{MED} in the media SAM of the storage media from the viewpoint of the security. At this time, the media key data K_{MED} is stored in the related media SAM when the media SAM is mounted in the storage media, while is stored in for example a region in the RAM region out of the management of the host CPU 810 when the media SAM is not mounted in the storage media.

[0517] Note that, as in the present embodiment, it is also possible that the mutual authentication be carried out between the apparatus side SAM (SAM 105_2 in the related example) and the media SAM (media SAM 252 in the related example), the media key data K_{MED} be transferred to the apparatus side SAM via the secure communication route, and the encryption and decryption using the media key data K_{MED} be carried out in the apparatus side SAM.

[0518] In the present embodiment, the storage key data K_{STR} and the media key data K_{MED} are used for protecting the security of the level of the physical layer of the storage media.

[0519] Further, the purchaser key data K_{PIN} is the data indicating the purchaser of the content file CF and is allocated to the related purchased user by the EMD service center 102 when the user purchases the content by for example a straight purchase. The purchaser key data K_{PIN} is managed in the EMD service center 102.

[0520] Step SK4: The media SAM manager 197 outputs the content file CF input from the SAM manager 190 and the key file KF_1 input from the encryptor/decryptor 173 to the storage module 260 shown in Fig. 26.

[0521] Then, the storage module 260 writes the content file CF and key file KF_1 input from the media SAM manager 197 into the RAM region 251 of the RAM type storage media 250 shown in Fig. 26. In this case, it is also possible that the key file KF_1 be written into the media SAM 252.

[0522] Below, the flow of the processing When determining the purchase mode in the AV apparatus 160_2 when a user home network 303 receives off-line the distribution of the ROM type storage medium 130 shown in Fig. 6 having the not yet determined purchase mode of the content will be explained by referring to Fig.32, Fig. 33, Fig. 34, and Fig. 35.

[0523] Step SL1: The SAM 105_2 of the AV apparatus 160_2 first performs the mutual authentication between the mutual authenticator 170 shown in Fig. 33 and the media SAM 133 of the ROM type storage media 130 shown in Fig. 6 and then receives as its input the media key data K_{MED} from the media SAM 133.

[0524] Note that, it is also possible that the related input not be carried out when the SAM 105_2 holds the media key data K_{MED} in advance.

[0525] Step SL2: The key file KF and signature data $SIG_{7,CP}$ thereof and the public key certificate data CER_{CP} and signature data $SIG_{1,ESC}$ thereof shown in Figs. 4B and 4C stored in the secure container 104 stored in the RAM region 132 of the ROM type storage media 130 are input via the media SAM manager 197 and are written into the stack memory 200.

[0526] Step SL3: The signature processor 189, after confirming the legitimacy of the signature data $SIG_{1,ESC}$, fetches the public key data $K_{CP,P}$ from public key certificate data CER_{CP} and verifies the legitimacy of the signature data $SIG_{7,CP}$, that is, the legitimacy of the creator of the key file KF, by using this public key data $K_{CP,P}$.

[0527] Step SL4: When the legitimacy of the signature data $SIG_{7,CP}$ is confirmed at the signature processor 189, the key file KF is read from the stack memory 200 to the secure container decryptor 183.

[0528] Then, the secure container decryptor 183 decrypts the key file KF by using the distribution key data KD_1 to KD_3 of the corresponding period.

[0529] Step SL5: The signature processor 189, after confirming the legitimacy of a signature data $SIG_{1,ESC}M$ stored in the key file KF by using the public key data $K_{ESC,P}$, verifies the legitimacy of the signature data $SIG_{2,CP}$ to $SIG_{4,CP}$, that is, the legitimacy of the creator of the content data C, content key data Kc ,and the usage control policy data 106, by using the public key data $K_{CP,P}$ stored in the public key certificate data CER_{CP} in the key file KF.

[0530] Step SL6: The charge processor 187 decides whether or not a control signal S165 indicating the trial listening mode was generated by the operation of the purchase/usage mode determination controller 165 shown in Fig. 16 by the user, and where the generation is decided, the processing of step SL7 is carried out, and while where the generation is not decided, the processing of step SL8 is carried out.

[0531] Step SL7: After the mutual authentication between the mutual authenticator 170 shown in Fig. 33 and the decryption/decompression module 163 shown in Fig. 32, the decryption/decompression module manager 184 of the SAM 105_2 outputs the content key data Kc stored in the stack memory 200, the semi-disclosure parameter data 199 stored in the usage control policy data 106, and the content data C read from the ROM region 131 of the ROM type storage media 130 to the decryption/decompression module 166 shown in Fig. 32. Next, the decryption/decompression module 163 decrypts the content data C in the semi-disclosure mode by using the content key data Kc and then decompresses it and outputs it to a reproduction module 270. Then, the reproduction medial 270 reproduces the content data C from the decryption/decompression module 163 in the trial listening mode.

[0532] Step SL8: The purchase mode of the content is determined by the purchase operation of the purchase mode determination controller 165 shown in Fig. 32 by

the user, then the control signal S165 indicating the related determined purchase mode is input to the charge processor 187.

[0533] Step SL9: The charge processor 187 generates the usage control status data 166 in response to the control signal S165 and writes this into the stack memory 200.

[0534] Further, the charge processor 187 generates or updates the usage log data 108.

[0535] Step SL10: For example, a new key file KF_1 shown in Fig. 29B storing the usage control status data 166 in the key file KF shown in Fig. 4B is output from the stack memory 200 to the encryptor/decryptor 173.

[0536] Step SL11: The encryptor/decryptor 173 sequentially encrypts the key file KF_1 shown in Fig. 29B read from the stack memory 200 by using the storage key data K_{STR}, media key data K_{MED}, and the purchaser key data K_{PIN} read from the storage unit 192 and outputs the same to the media SAM manager 197.

[0537] Step SL12: After the mutual authentication between the mutual authenticator 170 shown in Fig. 33 and the media SAM 133 shown in Fig. 32, the SAM manager 197 writes the key file KF_1 input from the encryptor/decryptor 173 via a storage module 271 shown in Fig. 32 into the RAM region 132 or the media SAM 133 of the ROM type storage media 130.

[0538] By this, the ROM type storage media 130 having the purchase mode determined is obtained.

[0539] At this time, the usage control status data 166 and the usage log data 108 generated by the charge processor 187 are read from the stack memory 200 and the external memory 201 at the predetermined timing and transmitted to the EMD service center 102.

[0540] Below, as shown in Fig. 36, an explanation will be made of the flow of the processing when reading the secure container 104 from the ROM type storage media 130 having the not yet determined purchase mode in the AV apparatus 160_3 and transferring the same to the AV apparatus 160_2, determining the purchase mode at the AV apparatus 160_2, and writing the same into RAM type storage media 250 by referring to Fig. 37 and Fig. 38.

[0541] Figure 37 is a flowchart of the related processing in the SAM 105_3.

[0542] Figure 38 is a flowchart of the related processing in the SAM 105_2. Note that, the secure container 104 may be transferred from the ROM type storage media 130 to the RAM type storage media 250 between the network apparatus 160_1 and any of the AV apparatuses 1602 to 160_4 shown in Fig. 1.

[0543] Step SM11 (Fig. 37): The mutual authentication is carried out between the SAM 105_3 of the AV apparatus 160_3 and the media SAM 133 of the ROM type storage media 130, then a media key data K_{MED1} of the ROM type storage media 130 is transferred to the SAM 105_3.

[0544] At this time, similarly, the mutual authentication is carried out between the SAM 105_2 of the AV apparatus 160_2 and a media SAM 252 of the RAM type storage media 250, then a media key data K_{MED2} of the RAM type storage media 250 is transferred to the SAM 105_2.

[0545] Step SM12: The SAM 105_3 sequentially decrypts the key file KF, the signature data $SIG_{7,CP}$, and the public key certificate data CER_{CP} and the signature data $SIG_{1,ESC}$ thereof of Figs. 4B and 4C read from the RAM region 132 in the encryptor/decryptor 172 shown in Fig. 40 by using the distribution key data KD_1 to KD_3 of the corresponding period.

[0546] Next, the content file CF decrypted in the encryptor/decryptor 172 is output to the encryptor/decryptor 171, encrypted by using the session key data K_{SES} obtained by the mutual authentication between the SAM 105_3 and 105_2, and then output to the SAM manager 190.

[0547] Further, the key file KF decrypted in the encryptor/decryptor 172 is output to the encryptor/decryptor 171 and the signature processor 189.

[0548] Step SM13: The signature processor 189 generates the signature data $SIG_{350,SAM3}$ of the key file KF by using the secret key data $K_{SAM3,S}$ of the SAM 105_3 and outputs this to the encryptor/decryptor 171.

[0549] Step SM14: The encryptor/decryptor 171 encrypts the public key certificate data CER_{SAM3} of the SAM 105_3 and the signature data $SIG_{351,ESC}$ thereof, the key file KF and the signature data $SIG_{350,SAM3}$ thereof read from the storage unit 192, and the content file CF shown in Fig. 4A read from the ROM region 131 of the ROM type storage media 130 by using the session key data K_{SES} obtained by the mutual authentication between the SAM 105_3 and 105_2 and then outputs the same to the SAM 105_2 of the AV apparatus 160_2 via the SAM manager 190.

[0550] Step SN1 (Fig. 38): In the SAM 105_2, as shown in Fig. 41, the content file CF input from the SAM 105_3 via the SAM manager 190 is decrypted by using the session key data K_{SES} in the encryptor/decryptor 171 and then written into a RAM region 251 of the RAM type storage media 250 via the media SAM manager 197.

[0551] Further, the key file KF and the signature data $SIG_{350,SAM3}$ thereof and the public key certificate data CER_{SAM3} and the signature data $SIG_{351,ESC}$ thereof input from the SAM 105_3 via the SAM manager 190 are written into the stack memory 200 and then decrypted by using the session key data K_{SES} in the encryptor/decryptor 171.

[0552] Step SN2: The related decrypted signature data $SIG_{351,ESC}$ is verified in the signature processor 189. When the legitimacy thereof is confirmed, the legitimacy of the signature data $SIG_{350,SAM3}$, that is, the legitimacy of the source of transmission of the key file KF, is confirmed by using the public key data K_{SAM3} stored in the public key certificate data CER_{SAM3}.

[0553] Then, when the legitimacy of the signature data $SIG_{350,SAM3}$ is confirmed, the key file KF is read from the stack memory 200 and output to the secure contain-

er decryptor 183.

[0554] Step SN3: The secure container decryptor 183 decrypts the key file KF by using the distribution key data KD_1 to KD_3 of the corresponding period and writes the related decrypted key file KF into the stack memory 200 after the predetermined signature verification.

[0555] Thereafter, the usage control policy data 106 stored in the key file KF already decrypted and stored in the stack memory 200 is output to the usage monitor 186. Then, the usage monitor 186 manages the purchase mode and the usage mode of the content based on the usage control policy data 106.

[0556] Step SN4: The charge processor 187 decides whether or not the control signal S165 indicating the trial listening mode is generated by the operation of the purchase/usage mode determination controller 165 of Fig. 16 by the user, performs the processing of step SN55 when it decides it is generated, and performs the processing of step SN6 when it is not generated.

[0557] Step SN5: When the trial listening mode is selected by the user, the content data C of the content file CF already decrypted by the session key data K_{SES}, the content key data Kc stored in the stack memory 200, the semi-disclosure parameter data 199, and the user watermark data 196 obtained from the usage control policy data 106 are output to the reproduction module 270 via the decryption/decompression module manager 184 shown in Fig. 36 after the mutual authentication. Then, the reproduction module 270 reproduces the content data C corresponding to the trial listening mode.

[0558] Step SN6: The purchase and/or usage mode of the content is determined by the operation of the purchase/usage determination controller 165 shown in Fig. 36 by the user, then the control signal S165 in accordance with the related determination is output to the charge processor 187.

[0559] Step SN7: The charge processor 187 generates the usage control status data 166 and the usage log data 108 in accordance with the determined purchase and/or usage mode and writes this into the stack memory 200 and the external memory 201.

[0560] Step SN8: For example, the key file KF_1 shown in Fig. 29B storing the usage control status data 166 read from the stack memory 200 is generated, then this is output to the encryptor/decryptor 173.

[0561] Step SN9: The encryptor/decryptor 173 sequentially encrypts the data by using the storage key data K_{STR}, media key data K_{MED2}, and the purchaser key data K_{PIN} read from the storage unit 192 and outputs it to the media SAM manager 197.

[0562] Step SN10: The media SAM manager 197 writes the key file KF_1 into the RAM region 251 or the media SAM 252 of the RAM type storage media 250 by the storage module 271 shown in Fig. 36.

[0563] Further, the usage control status data 166 and the usage log data 108 are transmitted to the EMD service center 102 at the predetermined timing.

[0564] Below, an explanation will be made of the method of realization of the SAMs 105_1 to 105_4.

[0565] When realizing the functions of the SAMs 105_1 to 105_4 as hardware, by using an ASIC type CPU including a memory, data having a high degree of secrecy such as the security functional module for realizing the functions shown in Fig. 17, the program module for performing the right clearing of the content, and the key data are stored in that memory. A series of right clearing use program modules such as an encryption library module (public key code, common key code, random number generator, hush function), a program module for the usage control of the content, and a program module of the charge processing are mounted as for example software.

[0566] For example, a module such as the encryptor/decryptor 171 shown in Fig. 17 is installed as an IP core in the ASIC type CPU as hardware due to the problem of for example processing speed. Depending to the clock speed or performance of CPU code system etc., it is also possible to install the encryptor/decryptor 171 as software.

[0567] Further, as the storage unit 192 shown in Fig. 17, the program module for realizing the functions shown in Fig. 17, and the memory for storing the data, use is made of for example a nonvolatile memory (flash-ROM), while as the working memory, a high speed writable memory such as an SRAM is used. Note that, other than them, as the memory included in the SAMs 105_1 to 105_4, it is also possible to use a ferroelectric memory (FeRAM).

[0568] Further, the SAMs 105_1 to 105_4 include, other than the above, a clock function used for the verification of the date in the term of validity and the contract period etc. for the usage of the content.

[0569] As mentioned above, the SAMs 105_1 to 105_4 have tamper resistant structures shutting off the program module, data, and the processing content from the outside. In order to prevent the program and content of data having high secrecy stored in the memory inside the IC of the related SAM or the values of the group of registers and the encryption library related to the system configuration of the SAMs or the group of registers of the clock from being read and newly written via the bus of the host CPU of the apparatuses with the SAMs 105_1 to 105_4 mounted thereon, that is, in order to prevent the host CPU of the mounted apparatus from accessing the allocated address space, each SAM sets an address space not visible from the host CPU of the mounted apparatus side using an MMU (memory management unit) for managing the memory space on the CPU side.

[0570] Further, the SAMs 105_1 to 105_4 have structures durable also against X-rays or heats or other physical attack from the outside and further have structures whereby even if real-time debugging (reverse engineering) using a debugging tool (hardware ICE, software ICE) or the like is carried out, the processing content cannot be understood or whereby a debugging tool per se cannot be used after the manufacture of ICs.

[0571] The SAMs 105_1 to 105_4 themselves are usual ASIC type CPUs including memories in the hardware structure. Their functions depend on the software for operating the related CPUs, but they differ from the general ASIC type CPUs in the point that they have encryption functions and tamper resistant hardware structures.

[0572] When realizing all of the functions of the SAMs 105_1 to 105_4 by software, there is the case where the software processing is carried out by enclosing the same inside a module having tamper resistance and the case where they are achieved by software processing on the host CPU mounted on a usual set and contrivances made to make deciphering impossible at only the time of the related processing. The former is the same as the case where the encryption library module is stored in the memory not as an IP core, but as a usual software module and can be considered similar to the case where it is realized as hardware. On the other hand, the latter is referred to as tamper resistant software whereby even if the state of execution can be deciphered by an ICE (debugger), the sequence of execution of a task is scattered (in this case, the task is cut so that each cut task piece has meaning as a program, that is, there is no influence upon the lines before and after that) or the task per se is encrypted and can be realized in the same way as a task scheduler (MiniOS) aimed at one type of secure processing. The related task scheduler is buried in the target program.

[0573] Next, an explanation will be made of the decryption/decompression module 163 shown in Fig. 16.

[0574] As shown in Fig. 16, the decryption/decompression module 163 has the mutual authenticator 220, decryptor 221, decryptor 222, decompression unit 223, electronic watermark information processor 224, and semi-disclosure processor 225.

[0575] The mutual authenticator 220 performs the mutual authentication with the mutual authenticator 170 shown in Fig. 26 and generates the session key data K_{SES} when the decryption/decompression module 163 receives as its input the data from the SAM 105_1.

[0576] The decryptor 221 decrypts the content key data Kc, semi-disclosure parameter data 199, user watermark data 196, and content data C input from the SAM 105_1 by using the session key data K_{SES}. Then, the decryptor 221 outputs the decrypted content key data Kc and the content data C to the decryptor 222, outputs the decrypted user watermark data 196 to the electronic watermark information processor 224, and outputs the semi-disclosure parameter data 199 to the semi-disclosure processor 225.

[0577] The decryptor 222 decrypts the content data C in the semi-disclosure state by using the content key data Kc under the control of the semi-disclosure processor 225 and outputs the decrypted content data C to the decompression unit 223.

[0578] The decompression unit 223 decompresses the decrypted content data C and outputs the same to the electronic watermark information processor 224.

[0579] The decompression unit 223 performs the decompression processing by using the A/V decompression software stored in the content file CF shown in Fig. 4A and performs the decompression processing by for example the ATRAC3 method.

[0580] The electronic watermark information processor 224 buries the user watermark in accordance with the decrypted user watermark data 196 in the decrypted content data C to generate new content data C. The electronic watermark information processor 224 outputs the related new content data C to the reproduction module 169.

[0581] In this way, the user watermark is buried at the decryption/decompression module 163 when reproducing the content data C.

[0582] Note that, in the present invention, it is also possible that the user watermark data 196 not be buried in the content data C.

[0583] The semi-disclosure processor 225 indicates the blocks not to be decrypted and the blocks to be decrypted in for example the content data C to the decryptor 222 based on the semi-disclosure parameter data 199.

[0584] Further, the semi-disclosure processor 225 performs control to for example limit the reproduction function at the time of trial listening or limit the possible listening period based on the semi-disclosure parameter data 199.

[0585] The reproduction module 169 performs the reproduction in accordance with the decrypted and decompressed content data C.

[0586] Next, an explanation will be made of the data format when transferring data with the signature data generated by using the secret key data attached thereto and public key certificate data among the content provider 101, EMD service center 102, and user home network 103.

[0587] Figure 42A is a view for explaining the data format for the case where the data Data is transmitted from the content provider 101 to the SAM 105_1 by the in-band method.

[0588] In this case, a module Mod_{50} encrypted by the session key data K_{SES} obtained by the mutual authentication between the content provider 101 and the SAM 105_1 is transmitted from the content provider 101 to the SAM 105_1.

[0589] The module Mod_{50} stores a module Mod_{51} and the signature data SIG_{CP} based on the secret key data $K_{CP,S}$ thereof.

[0590] The module Mod_{51} stores the public key certificate data CER_{CP} storing the secret key data $K_{CP,P}$ of the content provider 101, the signature data SIG_{ESC} obtained based on the secret key data $K_{ESC,S}$ with respect to the public key certificate data CER_{CP}, and the data Data to be transmitted.

[0591] In this way, by transmitting the module Mod_{50} storing the public key certificate data CER_{CP} from the content provider 101 to the SAM 105_1, when verifying

the signature data SIG_{CP} at the SAM 105_1, it becomes unnecessary to transmit the public key certificate data CER_{CP} from the EMD service center 102 to the SAM 105_1.

[0592] Figure 42B and Fig. 42C are views for explaining the data format in the case of transmitting the data Data from the content provider 101 to the SAM 105_1 by the out-of-band method.

[0593] In this case, a module Mod_{52} shown in Fig. 42B encrypted by the session key data K_{SES} obtained by the mutual authentication between the content provider 101 and the SAM 105_1 is transmitted from the content provider 101 to the SAM 105_1.

[0594] The module Mod_{52} stores the data Data to be transmitted and the signature data SIG_{CP} based on the secret key data $K_{CP,S}$ thereof.

[0595] Further, a module Mod_{53} shown in Fig. 42C encrypted by the session key data K_{SES} obtained by the mutual authentication between the EMD service center 102 and the SAM 105_1 is transmitted from the EMD service center 102 to the SAM 105_1.

[0596] The module Mod_{53} stores the public key certificate data CER_{CP} of the content provider 101 and the signature data SIG_{ESC} based on the secret key data $K_{ESC,S}$ thereof.

[0597] Figure 42D is a view for explaining the data format of the case where the data Data is transmitted from the SAM 105_1 to the content provider 101 by the in-band method.

[0598] In this case, a module Mod_{54} encrypted by the session key data K_{SES} obtained by the mutual authentication between the content provider 101 and the SAM 105_1 is transmitted from the SAM 105_1 to the content provider 101.

[0599] The module Mod_{54} stores a module Mod_{55} and the signature data SIG_{SAM1} based on the secret key data $K_{SAM1,S}$ thereof.

[0600] The module Mod_{55} stores the public key certificate data CER_{SAM1} storing the secret key data $K_{SAM1,P}$ of the SAM 105_1, the signature data SIG_{ESC} based on the secret key data $K_{ESC,S}$ with respect to public key certificate data CER_{SAM1}, and the data Data to be transmitted.

[0601] In this way, by transmitting the module Mod_{55} storing the public key certificate data CER_{SAM1} from the SAM 105_1 to the content provider 101, when verifying the signature data SIG_{SAM1} in the content provider 101, it becomes unnecessary to transmit the public key certificate data CER_{SAM1} from the EMD service center 102 to the content provider 101.

[0602] Figure 42E and Fig. 42F are views for explaining the data format when transmitting the data Data from the SAM 105_1 to the content provider 101 by the out-of-band method.

[0603] In this case, a module Mod_{56} shown in Fig. 42E encrypted by the session key data K_{SES} obtained by the mutual authentication between the content provider 101 and the SAM 105_1 is transmitted from the SAM 105_1 to the content provider 101.

[0604] The module Mod_{56} stores the data Data to be transmitted and the signature data SIG_{SAM1} based on the secret key data $K_{SAM1,S}$ thereof.

[0605] Further, a module Mod_{57} shown in Fig. 42F encrypted by a session key data K_{SES} obtained by the mutual authentication between the EMD service center 102 and the content provider 101 is transmitted from the EMD service center 102 to the content provider 101.

[0606] The module Mod_{57} stores the public key certificate data CER_{SAM1} of the SAM 105_1 and the signature data SIG_{ESC} based on the secret key data $K_{ESC,S}$ thereof.

[0607] Figure 43A is a view for explaining the data format when transmitting the data Data from the content provider 101 to the EMD service center 102 by the in-band method.

[0608] In this case, a module Mod_{58} encrypted by the session key data K_{SES} obtained by the mutual authentication between the content provider 101 and the EMD service center 102 is transmitted from the content provider 101 to the EMD service center 102.

[0609] The module Mod_{58} stores a module Mod_{59} and the signature data SIG_{CP} based on the secret key data $K_{CP,S}$ thereof.

[0610] The module Mod_{59} stores the public key certificate data CER_{CP} storing the secret key data $K_{CP,P}$ of the content provider 101, the signature data SIG_{ESC} based on the secret key data $K_{ESC,S}$ with respect to public key certificate data CER_{CP}, and the data Data to be transmitted.

[0611] Figure 43B is a view for explaining the data format when transmitting the data Data from the content provider 101 to the EMD service center 102 by the out-of-band method.

[0612] In this case, a module Mod_{60} shown in Fig. 43B encrypted by the session key data K_{SES} obtained by the mutual authentication between the content provider 101 and the EMD service center 102 is transmitted from the content provider 101 to the EMD service center 102.

[0613] The module Mod_{60} stores the data Data to be transmitted and the signature data SIG_{CP} based on the secret key data $K_{CP,S}$ thereof.

[0614] At this time, the public key certificate data CER_{CP} of the content provider 101 has been already registered in the EMD service center 102.

[0615] Figure 43C is a view for explaining the data format when transmitting the data Data from the SAM 105_1 to the EMD service center 102 by the in-band method.

[0616] In this case, a module Mod_{61} encrypted by the session key data K_{SES} obtained by the mutual authentication between the EMD service center 102 and the SAM 105_1 is transmitted from the SAM 105_1 to the EMD service center 102.

[0617] The module Mod_{61} stores a module Mod_{62} and the signature data SIG_{SAM1} based on the secret key data $K_{SAM1,S}$ thereof.

[0618] The module Mod_{62} stores the public key cer-

tificate data CER_{SAM1} storing the secret key data $K_{SAM1,P}$ of the SAM 105_1, the signature data SIG_{ESC} based on the secret key data $K_{ESC,S}$ with respect to public key certificate data CER_{SAM1}, and the data Data to be transmitted.

[0619] Figure 43D is a view for explaining the data format when transmitting the data Data from the SAM 105_1 to the EMD service center 102 by the out-of-band method.

[0620] In this case, a module Mod_{63} shown in Fig. 43D encrypted by the session key data K_{SES} obtained by the mutual authentication between the EMD service center 102 and the SAM 105_1 is transmitted from the SAM 105_1 to the EMD service center 102.

[0621] The module Mod_{63} stores the data Data to be transmitted and the signature data SIG_{SAM1} based on the secret key data $K_{SAM1,S}$ thereof.

[0622] At this time, the public key certificate data CER_{SAM1} of the SAM 105_1 has been already registered in the EMD service center 102.

[0623] Below, an explanation will be made of the processing for registration at the EMD service center 102 at the time of shipping of the SAMs 105_1 to 105_4.

[0624] Note that, the processing for registration of the SAMs 105_1 to 105_4 is the same, so the processing for registration of the SAM 105_1 will be explained below.

[0625] At the time of shipping of the SAM 105_1, the key data shown below is initially registered in the storage unit 192 shown in Fig. 17 etc. via the SAM manager 149 by the key server 141 of the EMD service center 102 shown in Fig. 11.

[0626] Further, the SAM 105_1 stores in the storage unit 192 etc., for example, at the time of shipping, the program etc. used when the SAM 105_1 accesses the EMD service center 102 the first time.

[0627] Namely, the storage unit 192 stores, for example, the identifier SAM_ID of the SAM 105_1 given the "*" on the left side in Fig. 21, the storage key data K_{STR}, the public key data $K_{R\text{-}CA}$ of the route certificate authority 2, the public key data $K_{ESC,P}$ of the EMD service center 102, the secret key data $K_{SAM1,S}$ of the SAM 105_1, the public key certificate data CER_{SAM1} and the signature data $SIG_{22,ESC}$ thereof, and the original key data for creating the authentication use key data between the decryption/decompression module 163 and the media SAM at the time of initial registration.

[0628] Note that, it is also possible to transmit the public key certificate data CER_{SAM1} from the EMD service center 102 to the SAM 105_1 when registering the same after the shipping of the SAM 105_1.

[0629] Here, the public key data KR-CA of the route certificate authority 2 uses an RSA generally used in electronic business transactions over the Internet etc. and has a data length of for example 1024 bits. The public key data $K_{R\text{-}CA}$ is issued by the route certificate authority 2 shown in Fig. 1.

[0630] The public key data $K_{ESC,P}$ of the EMD service center 102 is generated by utilizing an elliptical curve code having a short data length and a strength equivalent to the RSA or more and has a data length of for example 160 bits. Note that when considering the strength of the encryption, desirably the public key data $K_{ESC,P}$ has 192 bits or more. Further, the EMD service center 102 registers the public key data $K_{ESC,P}$ in the route certificate authority 92.

[0631] Further, the route certificate authority 92 generates the public key certificate data CER_{ESC} of the public key data $K_{ESC,P}$. The public key certificate data CER_{ESC} storing the public key data $K_{ESC,P}$ is preferably stored in the storage unit 192 at the time of shipping of the SAM 105_1. In this case, the public key certificate data CER_{ESC} is signed by the secret key data $K_{ROOT,S}$ of the route certificate authority 92.

[0632] The EMD service center 102 generates a random number to generate the secret key data $K_{SAM1,S}$ of the SAM 1 and generates the public key data $K_{SAM1,P}$ forming the pair together with this.

[0633] Further, the EMD service center 102 is given the authentication of the route certificate authority 92, issues the public key certificate data CER_{SAM1} of the public key data $K_{SAM1,P}$, and attaches the signature data to this by using its own secret key data $K_{ESC,S}$. Namely, the EMD service center 102 achieves the function of the second CA (certificate authority).

[0634] Further, the SAM 105_1 is allocated a unique identifier SAM_ID under the management of the EMD service center 102 by the SAM manager 149 of the EMD service center 102 shown in Fig. 11. This is stored in the storage unit 192 of the SAM 105_1 and, at the same time, stored also in the SAM database 149a shown in Fig. 11 and managed by the EMD service center 102.

[0635] Further, the SAM 105_1 is connected to the EMD service center 102 by for example the user after shipping for the registration procedure. At the same time, the distribution use public key data KD_1 to KD_3 are transferred from the EMD service center 102 to the storage unit 192.

[0636] Namely, the user utilizing the SAM 105_1 must perform the registration procedure at the EMD service center 102 before downloading the content. This registration procedure is performed off-line by for example mail by the user entering information identifying itself using for example a registration form attached when purchasing the apparatus with the SAM 105_1 mounted thereon (in the related example, the network apparatus 160_1).

[0637] The SAM 105_1 cannot be used until the registration procedure is passed.

[0638] The EMD service center 102 issues the identifier USER_ID unique to the user in accordance with the registration procedure of the SAM 105_1 by the user, manages the correspondence between the SAM_ID and the USER_ID in for example the SAM database 149a shown in Fig. 11, and utilizes the same at the time of charging.

[0639] Further, the EMD service center 102 allocates

the information reference use identifier ID and the password used at the first time to the user of the SAM 105_1 and notifies these to the user. The user can inquired about information for example the state of usage (usage log) of the content data up to the present at the EMD service center 102 by using the information reference use identifier ID and the password.

[0640] Further, the EMD service center 102 confirms the ID at the credit card company or the like and confirms the user off-line at the time of registration.

[0641] Next, as shown in Fig. 21, an explanation will be made of the procedure for storing the SAM registration list in the storage unit 192 inside the SAM 105_1.

[0642] The SAM 105_1 shown in Fig. 1 acquires the SAM registration list of the SAMs 105_1 to 105_4 present in its own system by utilizing a topology map generated when starting up the power of the apparatus connected to the bus 191 or connecting a new apparatus to the bus 191 when using for example an IEEE 1394 serial bus as the bus 191.

[0643] Note that, the topology map generated in accordance with the IEEE 1394 serial bus, that is, the bus 191, is generated to cover the SAMs 105_1 to 105_4 and the SCMS processing circuits 105_5 and 105_6 when, for example, as shown in Fig. 44, in addition to the SAM 105_1 to 105_4, the SCMS processing circuits 105_5 and 105_6 of the AV apparatuses 160_5 and 160_6 are connected to the bus 191.

[0644] Accordingly, the SAM 105_1 fetches the information for the SAMs 105_1 to 105_4 from the related topology map to generate the SAM registration list.

[0645] The data format of the SAM registration list is shown in for example Fig. 45.

[0646] Then, the SAM 105_1 registers the related SAM registration list in the EMD service center 102 and acquires a signature.

[0647] These processings are automatically carried out by the SAM 105_1 by utilizing the session of the bus 191. An instruction for registration of the SAM registration list is issued to the EMD service center 102.

[0648] The EMD service center 102 confirms the term of validity when receiving the SAM registration list shown in Fig. 45 from the SAM 105_1. Then, the EMD service center 102 sets up the corresponding portion by referring to the existence of the settlement function designated by the SAM 105_1 at the time of registration. Further, the EMD service center 102 checks the revocation list and sets a revocation flag in the SAM registration list. The revocation list is the list of the SAMs for which usage is prohibited (invalidated) by the EMD service center 102 for the reason of for example illicit usage.

[0649] Further, the EMD service center 102 fetches the SAM registration list corresponding to the SAM 105_1 at the time of settlement and confirms if the SAM described therein is contained in the revocation list. Further, the EMD service center 102 attaches a signature to the SAM registration list.

[0650] Note that the SAM revocation list is generated covering only the SAMs of the identical system (connected to the identical bus 191) and that the validity and invalidity of the related SAM are indicated by the revocation flag corresponding to each SAM.

[0651] Below, an explanation will be made of the overall operation of the content provider 101 shown in Fig. 1.

[0652] Figure 46 is a flowchart of the overall operation of the content provider 101.

[0653] Step S1: The EMD service center 102 transmits the public key certificate data CER_{CP} of the public key data K_{CP} of the content provider 101 to the content provider 101 after the content provider 101 passes through the predetermined registration processing.

[0654] Further, the EMD service center 102 transmits the certificate CER_{CP1} to CER_{CP4} of the public key data $K_{SAM1,P}$ to $K_{SAM4,P}$ of the SAMs 105_1 to 105_4 to the SAMs 105_1 to 105_4 after the SAMs 105_1 to 105_4 pass through the predetermined registration processing.

[0655] Further, the EMD service center 102 transmits six months' worth of the distribution key data KD_1 to KD_6 each having a term of validity of one month to the content provider 101 after the mutual authentication and transmits three months' worth of the distribution key data KD_1 to KD_3 to the user home network 103.

[0656] In this way, the EMD system 100 distributes the distribution key data KD_1 to KD_3 to the SAMs 105_1 to 105_4 in advance, therefore, even in the case where the SAMs 105_1 to 105_4 are off-line from the EMD service center 102, the secure container 104 distributed from the content provider 101 can be decrypted and purchased and used in the SAMs 105_1 to 105_4. In this case, the log of the related purchase and/or usage is described in the usage log data 108. The usage log data 108 is automatically transmitted to the EMD service center 102 when the SAMs 105_1 to 105_4 and the EMD service center 102 are connected. Therefore, the settlement processing in the EMD service center 102 can be reliably carried out. Note that the SAMs for which the usage log data 108 cannot be collected by the EMD service center 102 in a predetermined period are invalidated by the revocation list.

[0657] Note that the usage control status data 166 is transmitted from the SAMs 105_1 to 105_4 to the EMD service center 102 in real-time in principle.

[0658] Step S2: The content provider 101 transmits the right registration request module Mod_2 shown in Fig. 7A to the EMD service center 102 after the mutual authentication.

[0659] Then, the EMD service center 102 registers and authorizes the usage control policy data 106 and the content key data Kc after the predetermined signature verification.

[0660] Step S3: The content provider 101 performs the encryption by using the distribution key data KD_1 to KD_6 of the corresponding period etc., generates the content file CF and the key file KF shown in Figs. 4A and 4B, and distributes the secure container 104 storing them and public key certificate data CER_{CP} shown in

Fig. 4C to the user home network 103 on-line and/or off-line.

[0661] Step S4: The SAMs 105_1 to 105_4 of the user home network 103 decrypt the secure container 104 by using the distribution key data KD_1 to KD_3 of the corresponding period etc., verify the signature etc. for verifying the legitimacy of the creator and the transmitter of the secure container 104, and confirm whether or not the secure container 104 was transmitted from a legitimate content provider 101.

[0662] Step S5: The SAMs 105_1 to 105_4 determine the purchase and/or usage mode based on the control signal S165 in accordance with the operation of the purchase/usage mode determination controller 165 shown in Fig. 16 by the user.

[0663] At this time, the usage monitor 186 shown in Fig. 23 manages the purchase and/or usage mode of the content file CF by the user based on the usage control policy data 106 stored in the secure container 104.

[0664] Step S6: The charge processor 187 shown in Fig. 23 of each of the SAMs 105_1 to 105_4 generate the usage log data 108 and the usage control status data 166 describing the operation of the settlement of the purchase and/or usage mode by the user based on the control signal S165 and transmits the same to the EMD service center 102.

[0665] Step S7: The EMD service center 102 performs the settlement processing based on the usage log data 108 in the settlement processor 142 shown in Fig. 11 and generates the settlement claim data 152 and the settlement report data 107. The EMD service center 102 transmits the settlement claim data 152 and the signature data SIG_{88} thereof via the payment gateway 90 shown in Fig. 1 to the settlement organization 91. Further, the EMD service center 102 transmits the settlement report data 107 to the content provider 101.

[0666] Step S8: The settlement organization 91 verifies the signature data SIG_{88}, then distributes the money paid by the user to the owner of the content provider 101 based on the settlement claim data 152.

[0667] As explained above, the EMD system 100 distributes the secure container 104 of the mode shown in Fig. 4 from the content provider 101 to the user home network 103and performs the processing for the key file KF in the secure container 104 in the SAMs 105_1 to 105_4.

[0668] Further, the content key data Kc and the usage control policy data 106 stored in the key file KF are encrypted by using the distribution key data KD_1 to KD_3 and are decrypted inside only the SAMs 105_1 to 105_4 holding the distribution key data KD_1 to KD_3. Then, the SAMs 105_1 to 105_4 determine the purchase mode and the usage mode of the content data C based on the handling content of the content data C described in the usage control policy data 106 which a module having tamper resistance.

[0669] Accordingly, according to the EMD system 100, the purchase and usage of the content data C in the user home network 103 can be reliably carried out based on the content of the usage control policy data 106 generated by the related parties of the content provider 101.

[0670] Further, the EMD system 100 enables common right clearing of the content data C in the SAMs 105_1 to 105_4 both on-line and off-line by distributing the content data C from the content provider 101 to the user home network 103 by using the secure container 104 in both cases.

[0671] Further, the EMD system 100 enables use of common right clearing rules when purchasing, using, storing, and transferring the content data C in the network apparatus 160_1 and the AV apparatuses 160_2 to 160_4 in the user home network 103 by performing processing always based on the usage control policy data 106.

First Modification of First Embodiment

[0672] In the above embodiment, as shown in Fig. 4B, the case where the key file KF was encrypted by using the distribution key data KD in the content provider 101 and where the key file KF was decrypted by using the distribution key data KD in the SAMs 105_1 to 105_4 was illustrated, but the encryption of the key file KF using the distribution key data KD is not always necessary when the secure container 104 is directly supplied from the content provider 101 to the SAMs 105_1 to 105_4 as shown in Fig. 1.

[0673] In this way, the encryption of the key file KF by using the distribution key data KD exhibits a large effect when suppressing illegal action by the service provider by giving the distribution key data KD to only the content provider and the user home network when supplying content data from the content provider to the user home network via the service provider as in the second embodiment mentioned later.

[0674] Note that in the case of the first embodiment as well, the encryption of the key file KF by using the distribution key data KD is effective in the point of improving the ability to suppress illicit usage of the content data.

[0675] Further, in the above embodiment, the case where the suggested retailer' price data SRP was stored in the usage control policy data 106 in the key file KF shown in Fig. 4B was illustrated, but it is also possible to store the suggested retailer' price data SRP (price tag data) other than the key file KF in the secure container 104. In this case, the signature data generated by using the secret key data K_{CP} is attached to the suggested retailer' price data SRP.

Second Modification of First Embodiment

[0676] In the first embodiment, as shown in Fig. 1, the case where the EMD service center 102 performs the settlement processing in the settlement organization 91

via the payment gateway 90 by using the settlement claim data 152 generated by an apparatus itself was illustrated, but it is also possible to transmit for example the settlement claim data 152 from the EMD service center 102 to the content provider 101 as shown in Fig. 47 and have the content provider 101 itself perform the settlement processing with respect to the settlement organization 91 via the payment gateway 90 by using the settlement claim data 152.

Third Modification of First Embodiment

[0677] In the above first embodiment, the case where the secure container 104 was supplied from the single content provider 101 to the SAMs 105_1 to 105_4 of the user home network 103 was illustrated, but it is also possible to supply secure containers 104a and 104b from two or more content providers 101a and 101b to the SAMs 105_1 to 105_4.

[0678] Figure 48 is a view of the configuration of the EMD system according to a third modification of the first embodiment where the content providers 101a and 101b are used.

[0679] In this case, the EMD service center 102 distributes six months' worth of distribution key data KD_{a1} to KD_{a6} and KD_{b1} to KD_{b6} to the content providers 101a and 101b.

[0680] Further, the EMD service center 102 distributes three months' worth of the distribution key data KD_{a1} to KD_{a3} and KD_{b1} to KD_{b3} to the SAMs 105_1 to 105_4.

[0681] Further, the content provider 101a supplies the secure container 104a storing a content file CFa encrypted by using a unique content key data Kca and a key file KFa encrypting the content key data Kca and a usage control policy data 106a etc. by using the distribution key data KD_{a1} to KD_{a6} of the corresponding period to the SAMs 105_1 to 105_4 on-line and/or off-line.

[0682] At this time, as the identifier of the key file, use is made of the global unique identifier Content_ID distributed by the EMD service center 102. The content data is centrally managed by the EMD service center 102.

[0683] Further, the content provider 101b supplies the secure container 104b storing a content file CFb encrypted by using unique content key data Kcb and a key file KFb encrypting the content key data Kcb and usage control policy data 106b etc. by using the distribution key data KD_{b1} to KD_{b6} of the corresponding period to the SAMs 105_1 to 105_4 on-line and/or off-line.

[0684] The SAMs 105_1 to 105_4 decrypt the secure container 104a by using the distribution key data KD_{a1} to KD_{a3} of the corresponding period, determine the purchase mode of the content after the predetermined signature verification processing etc., and transmit usage log data 108a and usage control status data 166a generated in accordance with the related determined purchase mode and usage mode to the EMD service center 102.

[0685] Further, the SAMs 105_1 to 105_4 decrypt the secure container 104b by using the distribution key data KD_{b1} to KD_{b3} of the corresponding period, determine the purchase mode of the content after the predetermined signature verification processing etc., and transmit usage log data 108b and usage control status data 166b generated in accordance with the related determined purchase mode and usage mode to the EMD service center 102.

[0686] The EMD service center 102 generates settlement claim data 152a for the content provider 101a based on the usage log data 108a and performs the settlement processing with respect to the settlement organization 91 by using this.

[0687] Further, the EMD service center 102 generates settlement claim data 152b for the content provider 101b based on the usage log data 108b and performs the settlement processing with respect to the settlement organization 91 by using this.

[0688] Further, the EMD service center 102 performs the authorization by registering the usage control policy data 106a and 106b. At this time, the EMD service center 102 distributes the global unique identifier Content_ID with respect to the key files KFa and KFb corresponding to the usage control policy data 106a and 106b.

[0689] Further, the EMD service center 102 issues public key certificate data $CER_{CP}a$ and $CER_{CP}b$ of the content providers 101a and 101b and attaches its own signature data $SIG_{1b,ESC}$ and $SIG_{1a,ESC}$ to them to certify the legitimacy.

Second Embodiment

[0690] In the above embodiment, the case where the content data was directly distributed from the content provider 101 to the SAMs 105_1 to 105_4 of the user home network 103 was illustrated, but in the present embodiment, an explanation will be made of the case of distributing the content data provided by the content provider to the SAM of the user home network via the service provider.

[0691] Figure 49 is a view of the configuration of an EMD system 300 of the present embodiment.

[0692] As shown in Fig. 49, the EMD system 300 has a content provider 301, an EMD service center 302, a user home network 303, a service provider 310, a payment gateway 90, and a settlement organization 91.

[0693] The content provider 301, EMD service center 302, SAMs 105_1 to 105_4, and service provider 310 correspond to the data providing apparatus, management apparatus, data processing apparatus, and data distribution apparatus of the present invention.

[0694] The content provider 301 is the same as the content provider 101 of the first embodiment except for the point that it supplies the content data to the service provider 310.

[0695] Further, the EMD service center 302 is the

same as the EMD service center 102 of the first embodiment except for the point that the authentication function, key data management function, and right clearing function are provided also with respect to the service provider 310 in addition to the content provider 101 and SAMs 505_1 to 505_4.

[0696] Further, the user home network 303 has a network apparatus 360_1 and AV apparatuses 360_2 to 360_4. The network apparatus 3601 includes a SAM 305_1 and a CA module 311, while the AV apparatuses 360_2 to 360_4 include the SAMs 305_2 to 305_4.

[0697] Here, the SAMs 305_1 to 305_4 are the same as the SAMs 105_1 to 105_4 of the first embodiment except for the point that they receive the distribution of a secure container 304 from the service provider 310 and the point that they perform the verification processing of the signature data and the preparation of an SP use purchase log data (data distribution apparatus use purchase log data) 309 for the service provider 310 in addition to the content provider 301.

[0698] First, a brief explanation will be made of the EMD system 300.

[0699] In the EMD system 300, the content provider 301 transmits the usage control policy (UCP) data 106 similar to that of the first embodiment mentioned before indicating the content of the right such as the license conditions of the content data C of the content to be provided by itself to the authority manager having a high reliability, that is, the EMD service center 302. The usage control policy data 106 is registered in the EMD service center 302 and authorized (certified).

[0700] Further, the content provider 301 encrypts the content data C by the content key data Kc to generate the content file CF. Further, the content provider 301 encrypts the content key data Kc and the usage control policy data 106 by using the distribution key data KD_1 to KD_6 of the corresponding period distributed from the EMD service center 302 to generate the key file KF storing them. Then, the content provider 301 supplies the secure container 104 storing the content file CF, key file KF, and its own signature data to the service provider 310 by using the Internet or other network, a digital broadcast, storage medium, or an informal protocol or off-line or the like.

[0701] When receiving the secure container 104 from the content provider 301, the service provider 310 verifies the signature data and confirms if the secure container 104 was generated by a legitimate content provider 301 and the legitimacy of the sender.

[0702] Next, the service provider 310 generates price tag data (PT) 312 indicating the price obtained by adding the price of its service to the price (SRP) with respect to the content intended by the content provider 301 notified for example off-line.

[0703] Then, the service provider 310 generates the secure container 304 storing the content file CF and key file KF fetched from the secure container 104, the price tag data 312, and the signature data by its own secret key data $K_{SP,S}$ with respect to them.

[0704] At this time, the key file KF is encrypted by the distribution key data KD_1 to KD_6, and the service provider 310 does not hold the related distribution key data KD_1 to KD_6, therefore the service provider 310 cannot view or rewrite the content of the key file KF.

[0705] Further, the EMD service center 302 registers and authorizes the price tag data 312.

[0706] The service provider 310 distributes the secure container 304 to the user home network 303 on-line and/or off-line.

[0707] At this time, in the off-line case, the secure container 304 is supplied to the SAMs 305_1 to 305_4 as it is. On the other hand, in the on-line case, the mutual authentication is carried out between the service provider 310 and the CA module 311, the secure container 304 is encrypted by using the session key data K_{SES} in the service provider 310 and transmitted, and the secure container 304 received at the CA module 311 is decrypted by using the session key data K_{SES} and then transferred to the SAMs 305_1 to 305_4.

[0708] Next, the SAMs 305_1 to 305_4 decrypt the secure container 304 by using the distribution key data KD_1 to KD_3 of the corresponding period distributed from the EMD service center 302, then perform the verification processing of the signature data.

[0709] The secure container 304 supplied to the SAMs 305_1 to 305_4 is reproduced and stored in the storage medium after the purchase and/or usage mode is determined in accordance with the operation of the user in the network apparatus 360_1 and the AV apparatuses 360_2 to 360_4.

[0710] The SAMs 305_1 to 305_4 store the log of the purchase and/or usage of the secure container 304 as the usage log data 308.

[0711] The usage log data (log data or the management apparatus use log data) 308 is transmitted from the user home network 303 to the EMD service center 302 in response to for example a request from the EMD service center 302.

[0712] The EMD service center 302 determines (calculates) the charge content for each of the content provider 301 and the service provider 310 based on the usage log data 308 and performs the settlement at the settlement organization 91 such as the bank via the payment gateway 90 based on the results. By this, the money paid by the user of the user home network 103 is distributed to the content provider 101 and the service provider 310 by the settlement processing by the EMD service center 102.

[0713] In the present embodiment, in the same way as the first embodiment, by providing the content data C of digital by encapsulation, value can be imparted to the digital content itself by separating the conventional digital content, which had been closely attached to the storage medium, from the storage medium.

[0714] Here, the secure container is the most basic product capsule when selling the content data C (prod-

uct) no matter which distribution channel (delivery channel) it is provided over. Specifically, the secure container is a product capsule containing the encryption information for the charging, the signature data for verifying the legitimacy of the content of the content data C, the legitimacy of the party preparing the content data, and the legitimacy of the distributor of the content data, and information relating to the copyright such as the information concerning the electronic watermark information to be buried in the content data.

[0715] Further, in the present embodiment, the EMD service center 302 has the certificate authority function, key data management function, and the right clearing (profit distribution) function.

[0716] Namely, the EMD service center 302 plays the role of the second certificate authority with respect to the highest authority manager at the neutral position, that is, the route certificate authority 92, and certifies the legitimacy of the related public key data by attaching the signature based on the secret key data of the EMD service center 302 to public key certificate data of public key data to be used for the verification processing of the signature data in the content provider 301, service provider 310, and the SAMs 305_1 to 305_4. Further, as mentioned before, the registration and authorization of the usage control policy data 106 of the content provider 301 and the price tag data 312 of the service provider 310 are achieved by the certificate authority function of the EMD service center 302.

[0717] Further, the EMD service center 302 has a key data management function for managing for example the key data of the distribution key data KD_1 to KD_6.

[0718] Further, the EMD service center 302 has a right clearing (profit distribution) function of performing settlement with respect to the purchase and/or usage of the content by the user of the user home network 303 based on the usage control policy data 106 registered by the content provider 301, the usage log data 308 input from the SAMs 305_1 to 305_4, and the price tag data 312 registered by the service provider 310 and distributing and paying the money paid by the user to the content provider 301 and the service provider 310.

[0719] Below, the components of the content provider 301 will be explained in detail.

[Content Provider 301]

[0720] Figure 50 is a functional block diagram of the content provider 301 and shows the flow of the data related to the data transferred with the service provider 310.

[0721] As shown in Fig. 50, the content provider 301 has a content master source server 111, electronic watermark information adder 112, compressor 113, encryptor 114, random number generator 115, encryptor 116, signature processor 117, secure container generator 118, secure container database 118a, storage unit 119, mutual authenticator 120, encryptor/decryptor 121, usage control policy data generator 122, EMD service center manager 125, and service provider manager 324.

[0722] In Fig. 50, components given the same references as those of Fig. 2 are the same as the components of the same references explained in the first embodiment by referring to Fig. 2 and Fig. 3.

[0723] Namely, the content provider 301 has a configuration providing the service provider manager 324 in place of the SAM manager 124 shown in Fig. 2.

[0724] The service provider manager 324 provides the secure container 104 input from the secure container generator 118 to the service provider 310 shown in Fig. 49 off-line and/or on-line. The secure container 104, in the same way as the first embodiment, stores the content file CF and the signature data $SIG_{8,CP}$ thereof, the key file KF and the signature data $SIG_{7,CP}$ thereof, and the public key certificate data CER_{CP} and the signature data $SIG_{1,ESC}$ thereof shown in Fig. 4A, Fig. 4B and Fig. 4C.

[0725] When distributing the secure container 104 to the service provider 310 on-line, the service provider manager 324 encrypts the secure container 104 by using the session key data K_{SES} in the encryptor/decryptor 121 and then distributes the same via the network to the service provider 310.

[0726] Further, the flow of the data in the content provider 101 shown in Fig. 3 similarly applies also to the service provider 310.

[Service Provider 310]

[0727] The service provider 310 distributes the secure container 304 storing the content file CF and key file KF in the secure container 104 provided from the content provider 301 and the price tag data 312 generated by itself to the network apparatus 360_1 and the AV apparatuses 360_2 to 360_4 of the user home network 303 on-line and/or off-line.

[0728] The service modes of the distribution of content by the service provider 310 may be roughly classified into an independent service and a linked service.

[0729] An independent service is for example a service exclusively for download for individually distributing the content. Further, a linked service is a service for distributing content linked to a program and CM (advertisement). For example, content such as the theme song and insertion song of a drama is stored in the stream of the drama program. The user can purchase content such as the theme song and insertion song in the stream when watching the drama program.

[0730] Figure 51 is a functional block diagram of the service provider 310.

[0731] Note that, in Fig. 51, the flow of the data when supplying the secure container 304 in accordance with the secure container 104 supplied from the content provider 301 to the user home network 303 is shown.

[0732] As shown in Fig. 51, the service provider 310

has a content provider manager 350, a storage unit 351, a mutual authenticator 352, an encryptor/decryptor 353, a signature processor 354, a secure container generator 355, a secure container database 355a, a price tag data generator 356, a user home network manager 357, an EMD service center manager 358, and a user preference filter creator 920.

[0733] Below, an explanation will be made of the flow of the processing in the service provider 310 when creating the secure container 304 from the secure container 104 supplied from the content provider 301 and distributing this to the user home network 303 by referring to Fig. 51 and Fig. 52.

[0734] Figure 52 is a flowchart of the related processing.

[0735] Step SZ1: The content provider manager 350 receives the supply of the secure container 104 shown in Fig. 4 from the content provider 301 on-line and/or off-line and writes the secure container 104 into the storage unit 351.

[0736] At this time, the content provider manager 350 decrypts the secure container 104 in the encryptor/decryptor 353 by using the session key data K_{SES} obtained by the mutual authentication between the mutual authenticator 120 shown in Fig. 50 and the mutual authenticator 352 shown in Fig. 51 in the on-line case and then writes the same into the storage unit 351.

[0737] Step SZ2: The signature processor 354 verifies the signature data $SIG_{1,ESC}$ shown in Fig. 4C of the secure container 104 stored in the storage unit 351 by using the public key data $K_{ESC,P}$ of the EMD service center 302 read from the storage unit 351 and, after the legitimacy thereof is confirmed, fetches the public key data $K_{CP,P}$ from public key certificate data CER_{CP} shown in Fig. 4C.

[0738] Step SZ3: The signature processor 354 verifies the signature data $SIG_{8,CP}$ and $SIG_{7,CP}$ shown in Fig. 4A and Fig. 4B of the secure container 104 stored in the storage unit 351 by using the related fetched public key data $K_{CP,P}$.

[0739] Step SZ4: The price tag data generator 356 generates the price tag data 312 indicating the price obtained by adding the price of its own service to the price with respect to the content requested by the content provider 301 notified from for example the content provider 301 off-line and outputs this to the secure container generator 355.

[0740] Step SZ5: The signature processor 354 takes the hush values of the content file CF, key file KF, and price tag data 312, generates signature data $SIG_{62,SP}$, $SIG_{63,SP}$, and $SIG_{64,SP}$ by using a secret key data $K_{SP,P}$ of the service provider 310, and outputs the result to the secure container generator 355.

[0741] Step SZ6: The secure container generator 355 generates the secure container 304 storing the content file CF and the signature data $SIG_{62,SP}$ thereof, the key file KF and the signature data $SIG_{63,ESC}$ thereof, the price tag data 312 and the signature data $SIG_{64,SP}$ thereof, and the public key certificate data CER_{SP} and the signature data $SIG_{61,ESC}$ thereof shown in Fig. 53A to Fig. 53D and stores the same in the secure container database 355a. Then, the secure container generator 355 reads the secure container 304 in response to a request from the user home network 303 from the secure container database 355a and outputs the same to the user home network manager 357.

[0742] At this time, the secure container 304 may be a composite container storing a plurality of content files CF and a plurality of key files KF corresponding to them too. For example, it is also possible to store a plurality of content files CF concerning music, a video clip, a lyric card, liner notes, and a jacket in a single secure container 304. It is also possible that these plurality of content files CF etc. be stored in the secure container 304 with a directory structure.

[0743] Further, when the secure container 304 is transmitted by a digital broadcast, an MHEG (Multimedia and Hypermedia Information Coding Experts Group) protocol is used, while when it is transmitted by the Internet, an XML/SMIL/HTML (Hyper Text Markup Language) protocol is used.

[0744] At this time, the content file CF and the key file KF are centrally managed by the content provider 301 and do not depend on the protocol for transmitting the secure container 304. Namely, the content file CF and the key file KF are stored in the secure container 304 by tunneling the MHEG and HTML protocols.

[0745] Step SZ7: The user home network manager 357 supplies the secure container 304 to the user home network 303 off-line and/or on-line.

[0746] When distributing the secure container 304 to the network apparatus 360_1 of the user home network 303 on-line, the user home network manager 357 encrypts the secure container 304 by using the session key data K_{SES} in the encryptor/decryptor 352 after the mutual authentication and then distributes the same via the network to the network apparatus 360_1.

[0747] Note that, when broadcasting the secure container 304 via for example a satellite, the user home network manager 357 encrypts the secure container 304 by using scramble key data K_{SCR} or the like. Further, the scramble key data K_{SCR} is encrypted by using work key data K_w, while the work key data K_w is encrypted by using master key data K_M.

[0748] Then, the user home network manager 357 transmits the scramble key data K_{SCR} and the work key data K_W together with the secure container 304 to the user home network 303 via the satellite.

[0749] Further, for example it stores the master key data K_M in an IC card or the like and distributes the same to the user home network 303 off-line.

[0750] Further, when receiving the SP use purchase log data 309 concerning the content data C distributed by the related service provider 310 from the user home network 303, the user home network manager 357 writes this into the storage unit 351.

[0751] The service provider 310 refers to the SP use purchase log data 309 when determining the service content in the future. Further, the user preference filter creator 920 analyzes the preference of the users of the SAMs 305_1 to 305_4 transmitting the related SP use purchase log data 309 based on the SP use purchase log data 309 to generate anuser preference filter data 900 and transmits this via the user home network manager 357 to the CA module 311 of the user home network 303.

[0752] In Fig. 54, the flow of the data relating to the communication with the EMD service center 302 in the service provider 310 is shown.

[0753] Note that, as the prerequisite of the following processing, the related party of the service provider 310 performs processing for registration at the EMD service center 302 off-line by using for example its own ID card and bank account for the settlement processing and acquires the global unique identifier SP_ID. The identifier SP_ID is stored in the storage unit 351.

[0754] First, an explanation will be made of the processing when the service provider 310 requests the public key certificate data CER_{SP} for certifying the legitimacy of the public key data $K_{SP,S}$ corresponding to its own secret key data $K_{SP,S}$ to the EMD service center 302 by referring to Fig. 54.

[0755] First, the service provider 310 generates a random number by using the true random number generator to generate the secret key data $K_{SP,S}$, generates the public key data $K_{SP,S}$ corresponding to the related secret key data $K_{SP,S}$, and stores the same in the storage unit 351.

[0756] The identifiers SP_ID and the public key data $K_{SP,P}$ of the EMD service center manager 358 and the service provider 310 are read from the storage unit 351.

[0757] Then, the EMD service center manager 358 transmits the identifier SP_ID and the public key data $K_{SP,P}$ to the EMD service center 302.

[0758] Then, the EMD service center manager 348 receives as its inputs the public key certificate data CER_{SP} and the signature data $SIG_{61,ESC}$ thereof from the EMD service center 302 in accordance with the related registration and writes the same into the storage unit 351.

[0759] Next, an explanation will be made of the processing of the case where the service provider 310 registers the price tag data 312 in the EMD service center 302 and authorizes the same by referring to Fig. 54.

[0760] In this case, the signature processor 354 finds the hush value of a module Mod_{103} storing the price tag data 312 generated by the price tag data generator 356 and the global unique identifier Content_ID read from the storage unit 351 and generates the signature data $SIG_{80,SP}$ by using the secret key data $K_{SP,S}$.

[0761] Further, it reads the public key certificate data CER_{SP} and the signature data $SIG_{61,ESC}$ thereof from the storage unit 351.

[0762] Then, the encryptor/decryptor 353 encrypts a price tag registration request use module Mod_{102} shown in Fig. 55 by using the session key data K_{SES} obtained by the mutual authentication between the mutual authenticator 352 and the EMD service center 302, then transmits it from the EMD service center manager 358 to the EMD service center 302.

[0763] Note that, it is also possible that the global unique identifier SP_ID of the service provider 310 be stored in the module Mod_{103}.

[0764] Further, the EMD service center manager 358 writes settlement report data 307s received from the EMD service center 302 into the storage unit 351.

[0765] Further, the EMD service center manager 358 stores marketing information data 904 received from the EMD service center 302 in the storage unit 351.

[0766] The marketing information data 904 is used as a reference when the service provider 310 determines the content data C to be distributed from then on.

[EMD Service Center 302]

[0767] The EMD service center 302 plays a role as the certificate authority (CA), key management authority, and right clearing authority as mentioned before.

[0768] Figure 56 is a view of the configuration of the EMD service center 302.

[0769] As shown in Fig. 56, the EMD service center 302 has a key server 141, key database 141a, a settlement processor 442, a signature processor 443, a settlement organization manager 144, a certificate usage control policy manager 445, a CER database 445a, a content provider manager 148, a CP database 148a, a SAM manager 149, a SAM database 149a, a mutual authenticator 150, an encryptor/decryptor 151, a service provider manager 390, an SP database 390a, a user preference filter creator 901, and a marketing information data creator 902.

[0770] In Fig. 56, the functional blocks given the same references as those of Fig. 10 and Fig. 11 have substantially the same functions as those of the functional blocks having the same references explained in the first embodiment.

[0771] Below, an explanation will be made of the functional blocks given new references in Fig. 56.

[0772] Note that, in Fig. 56, the flow of the data related to the data transferred between the EMD service center 302 and the service provider 310 in the flow of the data among the functional blocks in the EMD service center 302 is shown.

[0773] Further, in Fig. 57, the flow of the data related to the data transferred between the EMD service center 302 and the content provider 301 in the flow of the data among the functional blocks in the EMD service center 302 is shown.

[0774] Further, in Fig. 58, the flow of the data related to the data transferred between the EMD service center 302 and the SAMs 305_1 to 305_4 shown in Fig. 49 and the settlement organization 91 in the flow of the data among the functional blocks in the EMD service center 302 is shown.

[0775] The settlement processor 442 performs the settlement processing based on the usage log data 308 input from the SAMs 305_1 to 305_4 and the suggested retailer' price data SPR and the price tag data 312 input from the certificate usage control policy manager 445 as shown in Fig. 58. Note that, at this time, the settlement processor 442 monitors the existence of dumping etc. by the service provider 310.

[0776] The settlement processor 442 generates settlement report data 307c and settlement claim data 152c for the content provider 301 as shown in Fig. 58 by the settlement processing and outputs them to the content provider manager 148 and the settlement organization manager 144.

[0777] Further, by the settlement processing, as shown in Fig. 56 and Fig. 58, it generates the settlement report data 307s and settlement claim data 152s for the service provider 310 and outputs them to the service provider manager 390 and the settlement organization manager 144.

[0778] Here, the settlement claim data 152c and 152s are authorized data enabling claim of payment of money to the settlement organization 91 based on the related data.

[0779] Here, the usage log data 308 is used when determining the payment of the license fee related to the secure container 304 in the same way as the usage log data 108 explained in the first embodiment. The usage log data 308, for example, as shown in Fig. 59, describes the identifier Content_ID of the content data C stored in the secure container 304, the identifier CP_ID of the content provider 301 providing the content data C stored in the. secure container 304, the identifier SP_ID of the service provider 310 distributing the secure container 304, the signal original data of the content data C, the compression method of the content data C in the secure container 304, the identifier Media_ID of the storage medium storing the secure container 304, the identifier SAM_ID of the SAMs 305_1 to 305_4 receiving the distribution of the secure container 304, and the USER_ID of the user of the related SAMs 105_1 to 105_4. Accordingly, in a case where the money paid by the user of the user home network 303 must be distributed to the license owners of for example the compression method and the storage medium other than the owners of the content provider 301 and the service provider 310, the EMD service center 302 determines the sum of money to be paid to the other parties based on the distribution rate table determined in advance and generates the settlement report data and settlement claim data in accordance with the related determination.

[0780] The certificate usage control policy manager 445 reads the public key certificate data CER_{CP}, public key certificate data CER_{SP}, public key certificate data CER_{SAM1} to CER_{SAM2}, etc. registered and authorized in the CER database 445a and registers and authorizes the usage control policy data 106 and content key data Kc of the content provider 301 and the price tag data 312 of the service provider 310 etc. in the CER database 445a.

[0781] At this time, the certificate usage control policy manager 445 takes the hush values of the usage control policy data 106, content key data Kc, price tag data 312, etc., attaches the signature data using the secret key data $K_{ESC,S}$, and thereby generates the authorized public key certificate data.

[0782] The content provider manager 148 has the function of communicating with the content provider 101 and can access the CP database 148a for managing the registered identifier CP_ID etc. of the content provider 101.

[0783] The user preference filter creator 901 generates user preference filter data 903 for selecting the content data C in accordance with the preference of the users of the SAMs 305_1 to 305_4 transmitting the related usage log data 308 based on the usage log data 308 and transmits the user preference filter data 903 to the SAMs 305_1 to 305_4 transmitting the related usage log data 308 via the SAM manager 149.

[0784] The marketing information data creator 902 generates the marketing information data 904 indicating the state of purchase etc. of the entire content data C distributed to the user home network 103 by for example a plurality of service providers 310 based on the usage log data 308 and transmits this via the service provider manager 390 to the service provider 310. The service provider 310 determines the content of the service to be provided from then on with the marketing information data 904 as a reference.

[0785] Below, an explanation will be made of the flow of the processing in the EMD service center 302.

[0786] The transmission of the distribution key data KD_1 to KD_6 from the EMD service center 302 to the content provider 301 and the transmission of the distribution key data KD_1 to KD_3 from the EMD service center 302 to the SAMs 305_1 to 305_4 are carried out in the same way as the case of the first embodiment.

[0787] Further, the processing in the case where the EMD service center 302 receives a request for issuance of public key certificate data from the content provider 301 is carried out in the same way as the case of the first embodiment except for the point that the certificate usage control policy manager 445 performs the registration with respect to the CER database 445a.

[0788] Below, an explanation will be made of the processing in the case where the EMD service center 302 receives a request for issuance of public key certificate data from the service provider 310 by referring to Fig. 56 and Fig. 60.

[0789] Figure 60 is a flowchart of the related processing.

[0790] Step SO1: When receiving a request for registration of public key certificate data containing the identifier SP_ID, public key data $K_{SP,P}$, and signature data $SIG_{70,SP}$ of the service provider 310 given by the EMD service center 302 in advance from the service provider

310, the service provider manager 390 decrypts them by using the session key data K_{SES} obtained by the mutual authentication between the mutual authenticator 150 and the mutual authenticator 352 shown in Fig. 51.

[0791] Step SO2: After confirming the legitimacy of the related decrypted signature data $SIG_{70,SP}$ at the signature processor 443, it is confirmed whether or not the service provider 310 issuing a request for issuance of the related public key certificate data is registered in the SP database 390a based on the identifier SP_ID and the public key data $K_{SP,P}$.

[0792] Step SO3: The certificate usage control policy manager 445 reads the public key certificate data CER_{SP} of the related service provider 310 from the CER database 445a and outputs the same to the service provider manager 390.

[0793] Step SO4: The signature processor 443 takes the hush value of the public key certificate data CER_{SP}, generates the signature data $SIG_{61,ESC}$ by using the secret key data $K_{ESC,S}$ of the EMD service center 302, and outputs this to the service provider manager 390.

[0794] Step SO5: The service provider manager 390 encrypts the public key certificate data CER_{SP} and the signature data $SIG_{61,ESC}$ thereof by using the session key data K_{SES} obtained by the mutual authentication between the mutual authenticator 150 and the mutual authenticator 352 shown in Fig. 51 and then transmits the same to the service provider 310.

[0795] Note that, the processing where the EMD service center 302 receives a request for issuance of public key certificate data from the SAMs 105_1 to 105_4 is similar to the first embodiment.

[0796] Further, also the processing where the EMD service center 302 receives the request for registration of the usage control policy data 106 from the content provider 301 is similar to that of the first embodiment.

[0797] Next, an explanation will be made of the processing where the EMD service center 302 receives the request for registration of the price tag data 312 from the service provider 310 by referring to Fig. 56 and Fig. 61.

[0798] Figure 61 is a flowchart of the related processing.

[0799] Step SP1: When the service provider manager 390 receives the price tag registration request module Mod_{102} shown in Fig. 55 from the service provider 310, it decrypts the price tag registration request module Mod_{102} by using the session key data K_{SES} obtained by the mutual authentication between the mutual authenticator 150 and the mutual authenticator 352 shown in Fig. 51.

[0800] Step SP2: The legitimacy of the signature data $SIG_{80,SP}$ stored in the related decrypted price tag registration request module Mod_{102} is confirmed in the signature processor 443.

[0801] Step SP3: The certificate usage control policy manager 445 registers and authorizes the price tag data 312 stored in the price tag registration request module Mod_{102} in the CER database 445a.

[0802] Next, an explanation will be made of the processing where the settlement is carried out in the EMD service center 302 by referring to Fig. 58 and Fig. 62.

[0803] Figure 62 is a flowchart of the related processing.

[0804] Step SQ1: When receiving as its inputs the usage log data 308 and signature data $SIG_{205,SAM1}$ thereof from for example the SAM 305_1 of the user home network 303, the SAM manager 149 decrypts the usage log data 308 and the signature data $SIG_{205,SAM1}$ by using the session key data K_{SES} obtained by the mutual authentication between the mutual authenticator 150 and the SAMs 305_1 to 305_4, verifies the signature data $SIG_{205,SAM1}$ by using the public key data $K_{SAM1,P}$ of the SAM 305_1, and then outputs the same to the settlement processor 442.

[0805] Step SQ2: The settlement processor 442 performs the settlement processing based on the usage log data 308 input from the SAM 305_1 and the suggested retailer' price data SRP and the price tag data 312 input from the certificate usage control policy manager 445.

[0806] The settlement processor 442 generates the settlement report data 307c and the settlement claim data 152c for the content provider 301 and the settlement report data 307s and the settlement claim data 152s for the service provider 310 as shown in Fig. 58 by the settlement processing.

[0807] Note that, it is also possible that the settlement processing by the settlement processor 442 be carried out whenever the usage log data 308 is input, and for every predetermined period.

[0808] Step SQ3: As shown in Fig. 56 and Fig. 58, the settlement claim data 152c and 152s for the content provider 301 and the service provider 310 are generated and output to the settlement organization manager 144.

[0809] The settlement organization manager 144 performs the mutual authentication of the settlement claim data 152c and 152s and the signature data generated for them by using the secret key data $K_{ESC,S}$ and the decryption by the session key data K_{SES} and then transmits the same to the settlement organization 91 via the payment gateway 90 shown in Fig. 49.

[0810] By this, the money of the sum indicated in the settlement claim data 152c is paid to the content provider 301, and the money of the sum indicated in the settlement claim data 152s is paid to the service provider 310.

[0811] Note that, it is also possible for the EMD service center 302 to transmit the settlement claim data 152c and 152s to the content provider 301 and the service provider 310. In this case, the content provider 301 and the service provider 310 claim the money to the settlement organization 91 based on the related received settlement claim data 152c and 152s.

[0812] Step SQ4: The settlement report data S307c and S307s for the content provider 301 and the service

provider 310 are output via the content provider manager 148 and the service provider manager 390 to the content provider 301 and the service provider 310.

[0813] The EMD service center 302 performs the processing at the time of shipping of the SAMs 305_1 to 305_4 and the registration processing of the SAM registration list in the same way as the EMD service center 102 of the first embodiment other than the above.

[User Home Network 303]

[0814] The user home network 303 has the network apparatus 3601 and the A/V apparatuses 360_2 to 360_4 as shown in Fig. 49.

[0815] The network apparatus 360_1 includes the CA module 311 and the SAM 305_1. Further, the A/V apparatuses 360_2 to 360_4 include the SAMs 305_2 to 305_4.

[0816] The SAMs 305_2 to 305_4 are connected to each other via the bus 191, for example, a IEEE serial interface bus.

[0817] Note that it is also possible that the AV apparatuses 360_2 to 360_4 have a network communication function or do not have a network communication function, but utilize the network communication function of the network apparatus 360_1 via the bus 191.

[0818] Further, it is also possible that the user home network 303 have only AV apparatuses not having the network function.

[0819] Below, an explanation will be made of the network apparatus 360_1.

[0820] Figure 63 is a view of the configuration of the network apparatus 360_1.

[0821] As shown in Fig. 63, the network apparatus 360_1 has a communication module 162, a CA module 311, a decryption module 905, a SAM 305_1, a decryption/decompression module 163, a purchase/usage mode determination controller 165, a download memory 167, a reproduction module 169, and an external memory 201.

[0822] In Fig. 63, components given the same references as those of Fig. 16 are the same as the components of the same references explained in the first embodiment.

[0823] The communication module 162 performs the communication processing with the service provider 310.

[0824] Specifically, the communication module 162 outputs the secure container 304 received from the service provider 310 by a satellite broadcast or the like to the decryption module 905. Further, the communication module 162 outputs the user preference filter data 900 receiving the SP use purchase log data 309 via a telephone line or the like at the service provider 310 to the CA module 311 and, at the same time, transmits the SP use purchase log data 309 input from the CA module 311 to the service provider 310 via a telephone line or the like.

[0825] Figure 64 is a functional block diagram of the CA module 311 and the decryption module 905.

[0826] As shown in Fig. 64, the CA module 311 has a mutual authenticator 906, a storage unit 907, an encryptor/decryptor 908, and an SP use purchase log data creator 909.

[0827] When transferring data between the CA module 311 and the service provider 310 via the telephone line, the mutual authenticator 906 performs the mutual authentication with the service provider 310 to generate the session key data K_{SES} and outputs this to the encryptor/decryptor 908.

[0828] The storage unit 907 stores the master key data K_M supplied from the service provider 310 off-line by using an IC card 912 etc. after for example a contract is established between the service provider 310 and the user.

[0829] The encryptor/decryptor 908 receives as its inputs the encrypted scramble key data K_{SCR} and work key data K_w from a decryptor 910 of the decryption module 905 and decrypts the work key data K_W by using the master key data K_M read from the storage unit 907. Then, the encryptor/decryptor 908 decrypts the scramble key data K_{SCR} by using the related decrypted work key data K_W and outputs the related decrypted scramble key data K_{SCR} to the decryptor 910.

[0830] Further, the encryptor/decryptor 908 decrypts the user preference filter data 900 received by the communication module 162 from the service provider 310 via a telephone line or the like by using the session key data K_{SES} from the mutual authenticator 906 and outputs the same to a secure container selector 911 of the decryption module 905.

[0831] Further, the encryptor/decryptor 908 decrypts the SP use purchase log data 309 input from the SP use purchase log data creator 909 by using the session key data K_{SES} from the mutual authenticator 906 and transmits the same via the communication module 162 to the service provider 310.

[0832] The SP use purchase log data creator 909 generates the SP use purchase log data 309 indicating the purchase log of the content data C inherent in the service provider 310 based on the control signal S165 in accordance with the purchase operation of the content data C by the user by using the purchase/usage mode determination controller 165 shown in Fig. 63 or the usage control status data 166 from the SAM 305_1 and outputs this to the encryptor/decryptor 908.

[0833] The SP use purchase log data 309 contains for example the information to be collected from the user concerning the distribution service by the service provider 310, monthly base fee (network rent), contract (update) information, and the purchase log information.

[0834] Note that, the CA module 311 communicates with a charge database, a customer management database, and a marketing information database of the service provider 310 when the service provider 310 has the charge function. In this case, the CA module 311 transmits the charge data for the distribution service of the

content data to the service provider 310.

[0835] The decryption module 905 has the decryptor 910 and the secure container selector 911.

[0836] The decryptor 910 receives as its inputs the encrypted secure container 304, scramble key data K_{SCR}, and the work key data K_W from the communication module 162.

[0837] Then, the decryptor 910 outputs the encrypted scramble key data K_{SCR} and work key data K_w to the encryptor/decryptor 908 of the CA module 311 and receives as its input the decrypted scramble key data K_{SCR} from the encryptor/decryptor 908.

[0838] Then, the decryptor 910 decrypts the encrypted secure container 304 by using the scramble key data K_{SCR} and then outputs the same to the secure container selector 911.

[0839] Note that, when the secure container 304 is transmitted from the service provider 310 by the MPEG2 Transport Stream system, for example, the decryptor 910 fetches the scramble key data K_{SCR} from an ECM (Entitlement Control Message) in a TS packet and fetches the work key data K_W from an EMM (Entitlement Management Message).

[0840] The ECM, other than the above, contains for example program attribute information for every channel. Further, the EMM, other than this, contains individual trial listening contract information different for every user (auditor) etc.

[0841] The secure container selector 911 filters the secure container 304 input from the decryptor 910 by using the user preference filter data 900 input from the CA module 311, selects the secure container 304 in accordance with the preference of the user, and outputs the same to the SAM 305_1.

[0842] Next, an explanation will be made of the SAM 305_1. Note that, the SAM 305_1 has basically the same function and structure as the SAM 105_1 of the first embodiment mentioned before by using Fig. 17 to Fig. 41 except it performs the processing concerning the service provider 310 in addition to the content provider 310, for example, it performs the signature verification processing for the service provider 310.

[0843] Further, the SAMs 305_2 to 305_4 basically have the same functions as those of the SAM 305_1.

[0844] Namely, the SAMs 305_1 to 305_4 are modules for performing the charge processing in units of content and communicate with the EMD service center 302.

[0845] Below, the functions of the SAM 305_1 will be explained in detail.

[0846] Figure 65 is a view of the configuration of the SAM 305_1.

[0847] Note that, in Fig. 65, the flow of the data related to the processing of receiving as the input the secure container 304 from the service provider 310 and decrypting the key file KF in the secure container 304 is shown.

[0848] As shown in Fig. 65, the SAM 305_1 has a mutual authenticator 170, encryptor/decryptors 171, 172, and 173, error corrector 181, download memory manager 182, secure container decryptor 183, decryption/decompression module manager 184, EMD service center manager 185, usage monitor 186, signature processor 189, SAM manager 190, storage unit 192, media SAM manager 197, stack memory 200, service provider manager 580, charge processor 587, signature processor 598, and external memory manager 811.

[0849] Note that, the predetermined functions of the SAM 305_1 shown in Fig. 65 are realized by executing a secret program in the CPU in the same way as the case of the SAM 105_1.

[0850] In Fig. 65, functional blocks given the same references as those of Fig. 17 are the same as the functional blocks having the same references explained in the first embodiment.

[0851] Further, the external memory 201 shown in Fig. 63 stores the usage log data 308 and the SAM registration list after the processing explained in the first embodiment and the processing mentioned later.

[0852] Further, the stack memory 200, as shown in Fig. 66, stores the content key data Kc, usage control policy data (UCP) 106, lock key data K_{LOC} of the storage unit 192, public key certificate data CER_{CP} of the content provider 301, public key certificate data CER_{SP} of the service provider 310, usage control status data (UCS) 366, SAM program download containers SDC_1 to $SFDC_3$, price tag data 312, etc.

[0853] Below, an explanation will be made of the functional blocks newly given references in Fig. 65 among the functional blocks of the SAM 305_1.

[0854] The signature processor 589 verifies the signature data in the secure container 304 by using the public key data $K_{ESC,P}$ of the EMD service center 302, public key data $K_{CP,P}$ of the content provider 301, and the public key data $K_{SP,P}$ of the service provider 310 read from the storage unit 192 or the stack memory 200.

[0855] The charge processor 587 performs the charge processing in accordance with the purchase and/or usage mode of the content by the user based on the control signal S165 from the purchase/usage mode determination controller 165 shown in Fig. 63 and the price tag data 312 read from the stack memory 200 as shown in Fig. 67.

[0856] The charge processing by the charge processor 587 is carried out based on the content of the right such as the license conditions indicated by the usage control policy data 106 and the usage control status data 166 under the monitoring of the usage monitor 186. Namely, the user can purchase and use the content within the range according to the related content of the right etc.

[0857] Further, the charge processor 587 generates the usage log data 308 in the charge processing and writes this into the external memory 201 via the external memory manager 811.

[0858] Here, the usage log data 308 is used when determining the payment of the license fee related to the

secure container 304 in the EMD service center 302 in the same way as the usage log data 108 of the first embodiment.

[0859] Further, the charge processor 587 generates the usage control status (UCS) data 166 describing the purchase and/or usage mode of the content by the user based on the control signal S165 and writes this into the external memory 201 via the external memory manager 811.

[0860] As the purchase modes of the content, there are for example a straight purchase without restriction as to reproduction by the purchaser and copying for the usage of the related purchaser and a reproduction charge charging whenever it is reproduced.

[0861] Here, the usage control status data 166 is generated when the user determines the purchase mode of the content, then is used for control so that the user uses the related content within the range permitted by the related determined purchase mode. The usage control status data 166 describes the ID of the content, the purchase mode, the straight purchase price, the SAM_ID of the SAM with the purchase of the related content performed therefor, USER_ID of the purchasing user, etc.

[0862] Note that, when the determined purchase mode is the reproduction charge, for example, the usage control status data 166 is transmitted from the SAM 305_1 to the service provider 310 in real-time, and the service provider 310 indicates to the EMD service center 302 to take the usage log data 108 from the SAM 105_1.

[0863] Further, when the determined purchase mode is a straight purchase, for example, the usage control status data 166 is transmitted to the service provider 310 and the EMD service center 302 in real-time.

[0864] Further, the SAM 305_1 outputs the user preference filter data 903 received by the EMD service center manager 185 from the EMD service center 302 to the service provider manager 580. Then, the service provider manager 580 filters the secure container 304 input from the decryption module 905 shown in Fig. 63 based on the user preference filter data 903, selects the secure container 304 in accordance with the preference of the user, and outputs the related selected secure container 304 to the error corrector 181. By this, the SAM 305_1 can perform the processing for selection of the content data C based on the preference of the related user obtained from the state of purchase of the content data C by the related user covering all service providers 310 contracted with the user of the related SAM 305_1.

[0865] Below, the flow of the processing in the SAM 305_1 will be explained.

[0866] The flow of the processing when storing the distribution key data KD_1 to KD_3 received from the EMD service center 302 in the storage unit 192 is similar to that of the case of the SAM 105_1 mentioned before.

[0867] Below, an explanation will be made of the flow of the processing in the SAM 305_1 when receiving as its input the secure container 304 from the service provider 310 and decrypting the key file KF in the secure container 304 by referring to Fig. 65 and Fig. 68.

[0868] Figure 68 is a flowchart of the related processing. Step SR1: The mutual authentication is carried out between the mutual authenticator 170 and the mutual authenticator 352 of the service provider 310 shown in Fig. 51.

[0869] The encryptor/decryptor 171 decrypts the secure container 304 shown in Fig. 53A to Fig. 53D received from the service provider 310 via the service provider manager 580 by using the session key data K_{SES} obtained by the related mutual authentication.

[0870] Step SR2: The signature processor 589 verifies the signature data $SIG_{61,ESC}$ shown in Fig. 53D and then confirms the legitimacy of the signature data $SIG_{62,SP}$, $SIG_{63,SP}$, and $SIG_{64,SP}$ by using the public key data $_{KSP,P}$ of the service provider 310 stored in the public key certificate data CER_{SP} shown in Fig. 53D.

[0871] When the legitimacy of the signature data $SIG_{62,SP}$, $SIG_{63,SP}$, and $SIG_{64,SP}$ is confirmed, the service provider manager 580 outputs the secure container 304 to the error corrector 181.

[0872] The error corrector 181 corrects the error of the secure container 304 and then outputs the result to the download memory manager 182.

[0873] Step SR3: The download memory manager 182 performs the mutual authentication between the mutual authenticator 170 and the media SAM 167a shown in Fig. 63 and then writes the secure container 304 into the download memory 167.

[0874] Step SR4: The download memory manager 182 performs the mutual authentication between the mutual authenticator 170 and the media SAM 167a shown in Fig. 63 and then reads the key file KF shown in Fig. 53B stored in the secure container 304 and outputs the same to the secure container decryptor 183.

[0875] Then, the secure container decryptor 183 decrypts the key file KF by using the distribution key data KD_1 to KD_3 of the corresponding period input from the storage unit 192.

[0876] Step SR5: The secure container decryptor 183 outputs the signature data $SIG_{1,ESC}$ and $SIG_{2,CP}$ to $SIG_{4,CP}$ stored in the signature certificate module Mod_1 shown in Fig. 53B to the signature processor 589.

[0877] The signature processor 589 verifies the signature data $SIG_{1,ESC}$ shown in Fig. 53B and then verifies the signature data $SIG_{2,CP}$ to $SIG_{4,CP}$ by using the public key data $K_{CP,P}$ stored in public key certificate data CER_{CP}.

[0878] Step SR6: The secure container decryptor 183 writes the key file KF into the stack memory 200 when the legitimacy of the signature data $SIG_{2,CP}$ to $SIG_{4,CP}$ is confirmed.

[0879] Below, an explanation will be made of the flow of the processing until the purchase mode of the secure container 304 downloaded from the service provider 310 on the download memory 167 is determined by referring to Fig. 67 and Fig. 69.

[0880] Figure 69 is a flowchart of the related process-

ing. Step SS1: The charge processor 587 decides by the operation of the purchase/usage mode determination controller 165 shown in Fig. 63 by the user whether or not the control signal S165 indicating the trial listening mode was input. Where it decides it was input, it executes the processing of step SS2, while when it decides it was not input, executes the processing of step SS3.

[0881] Step SS2: For example, the content file CF stored in the download memory 167 is output to the decryption/decompression module 163 shown in Fig. 63 via the decryption/decompression module manager 184.

[0882] At this time, with respect to the content file CF, the mutual authentication between the mutual authenticator 170 and the media SAM 167a, the encryption and/or decryption by the session key data K_{SES}, the mutual authentication between the mutual authenticator 170 and the mutual authenticator 220, and the encryption and/or decryption by the session key data K_{SES} are carried out.

[0883] The content file CF is decrypted in the decryptor 221 shown in Fig. 63 and then output to the decryptor 222.

[0884] Further, the content key data Kc and semi-disclosure parameter data 199 read from the stack memory 200 are output to the decryption/decompression module 163 shown in Fig. 63. At this time, after the mutual authentication between the mutual authenticator 170 and the mutual authenticator 220, the encryption and decryption by the session key data K_{SES} are carried out with respect to the content key data Kc and the semi-disclosure parameter data 199.

[0885] Next, the decrypted semi-disclosure parameter data 199 is output to the semi-disclosure processor 225, and the decryption of the content data C using the content key data Kc by the decryptor 222 is carried out by semi-disclosure under the control from the semi-disclosure processor 225.

[0886] Next, the content data C decrypted by semi-disclosure is decompressed at the decompression unit 223 and then output to the electronic watermark information processor 224.

[0887] Next, he user watermark data 196 is buried in the content data C in the electronic watermark information processor 224, then the content data C is reproduced at the reproduction module 169, and the audio in accordance with the content data C is output.

[0888] Step SS3: When the user trying out the content determines the purchase mode by operating the purchase/usage mode determination controller 165, the control signal S165 indicating the related determined purchase mode is output to the charge processor 187.

[0889] Step SS4: The charge processor 187 generates the usage log data 308 and the usage control status data 166 in accordance with the determined purchase mode, writes the usage log data 308 into the external memory 201 via the external memory manager 811, and writes the usage control status data 166 into the stack memory 200.

[0890] Below, the usage monitor 186 performs control (monitor) so that the purchase and usage of the content are carried out within the range permitted by the usage control status data 166.

[0891] Step SS5: The usage control status data 166 is added to the key file KF stored in the stack memory 200, and a new key file KF_{11} shown in Fig. 71 having the determined purchase mode is generated. The key file KF_{11} is stored in the stack memory 200.

[0892] As shown in Fig. 71, the usage control status data 166 stored in the key file KF1 is encrypted by utilizing the CBC mode of the DES by using the session key data K_{STR}. Further, the MAC value generated by using the related storage key data K_{STR} as the MAC key data, that is, the MAC_{300}, is attached. Further, the module comprised by the usage control status data 166 and the MAC_{300} is been encrypted by utilizing the CBC mode of DES by using the media key data K_{MED}. Further, a MAC value generated by using the related media key data K_{MED} as the MAC key data, that is, the MAC_{301}, is attached to the related module.

[0893] Next, an explanation will be made of the flow of the processing in the case where the content data C having the purchase mode already determined stored in the download memory 167 is reproduced by referring to Fig. 67 and Fig. 70.

[0894] Figure 70 is a flowchart of the related processing. Step ST1: For example, in accordance with the operation by the user, the designation of the content to be reproduced is received at the SAM.

[0895] Step ST2: Under the monitoring of the usage monitor 186, the content file CF stored in the download memory 167 is read based on the control signal S165.

[0896] Step ST3: The related read content file CF is output to the decryption/decompression module 163 shown in Fig. 63.

[0897] Further, the content key data Kc read from the stack memory 200 is output to the decryption/decompression module 163.

[0898] Step ST4: The decryptor 222 of the decryption/decompression module 163 decrypts the content file CF using the content key data Kc and the decompression processing by the decompression unit 223 and reproduces the content data C at the reproduction module 169.

[0899] Step ST5: The charge processor 587 updates the usage log data 308 in accordance with the control signal S165.

[0900] The usage log data 308 is transmitted together with the signature data $SIG_{205,SAM1}$ generated by using the secret key data $_{KSAM1,S}$ to the EMD service center 302 via the EMD service center manager 185 at the predetermined timing.

[0901] Below, an explanation will be made of the flow of the processing in the SAM 305_1 in the case of, as shown in Fig. 72, transferring for example the content file CF having the purchase mode already determined

and downloaded in the download memory 167 of the network apparatus 3601 to the SAM 305_2 of the AV apparatus 3602 via the bus 191 by referring to Fig. 73 and Fig. 74.

[0902] Step SU1: The user operates the purchase/usage mode determination controller 165 and indicates to this to transfer the predetermined content stored in the download memory 167 to the AP apparatus 360_2 and outputs the control signal S165 in response to the related operation to the charge processor 587.

[0903] By this, the charge processor 587 updates the usage log data 308 stored in the stack memory 200 based on the control signal S165.

[0904] Step SU2: The download memory manager 182 outputs the content file CF shown in Fig. 75A read from the download memory 167 to the SAM manager 190.

[0905] Step SU3: The key file KF_{11} having the purchase mode already determined shown in Fig. 75B read from the stack memory 200 is output to the signature processor 589 and the SAM manager 190.

[0906] Step SU4: The signature processor 589 generates the signature data $SIG_{80,SAM1}$ of the key file KF_{11} and outputs this to the SAM manager 190.

[0907] Step SU5: The SAM manager 190 reads the public key certificate data CER_{SAM1} shown in Fig. 75C and the signature data $SIG_{22,ESC}$ thereof from the storage unit 192.

[0908] Further, the mutual authenticator 170 outputs the session key data K_{SES} obtained by performing the mutual authentication with the SAM 305_2 to the encryptor/decryptor 171.

[0909] The SAM manager 190 generates the secure container comprised by the data shown in Figs. 75A, 75B, and 75C.

[0910] Step SU6: The encryptor/decryptor 171 encrypts and generates the related secure container by using the session key data K_{SES} and outputs it to the SAM 305_2 of the AV apparatus 360_2 shown in Fig. 73.

[0911] Below, an explanation will be made of the flow of the processing in the SAM 305_2 when writing the content file CF etc. input from the SAM 305_1 into a RAM type storage medium or the like by referring to Fig. 76 and Fig. 77.

[0912] Figure 77 is a flowchart of the related processing. Step SV1: The SAM manager 190 of the SAM 305_2 receives as its inputs the content file CF shown in Fig. 75A, the key file KF_{11} and the signature data $SIG_{80,SAM1}$ thereof shown in Fig. 75B, and the public key certificate data CER_{SAM1} and the signature data $SIG_{22,ESC}$ thereof shown in Fig. 75C from the SAM 305_1 of the network apparatus 360_1 as shown in Fig. 76.

[0913] Then, the encryptor/decryptor 171 decrypts the content file CF, the key file KF_{11} and the signature data $SIG_{80,SAM1}$ thereof, the public key certificate data CER_{SAM1} and the signature data $SIG_{22,ESC}$ thereof received by the SAM manager 190 as inputs by using the session key data K_{SES} obtained by the mutual authentication between the mutual authenticator 170 and the mutual authenticator 170 of the SAM 305_1.

[0914] Next, the content file CF decrypted by using the session key data K_{SES} is output to the media SAM manager 197.

[0915] Further, the key file KF_{11} and the signature data $SIG_{80,SAM1}$ thereof and the public key certificate data CER_{SAM1} and the signature data $SIG_{22,ESC}$ thereof decrypted by using the session key data K_{SES} are written into the stack memory 200.

[0916] Step SV2: The signature processor 589 verifies the signature data $SIG_{22,ESC}$ read from the stack memory 200 by using the public key data $K_{ESC,P}$ read from the storage unit 192 and confirms the legitimacy of the public key certificate data CER_{SAM1}.

[0917] Then, the signature processor 589 confirms the legitimacy of the signature data $SIG_{80,SAM1}$ by using the public key data $K_{SAM1,P}$ stored in the public key certificate data CER_{SAM1} when confirming the legitimacy of the public key certificate data CER_{SAM1}.

[0918] Step SV3: When the legitimacy of the signature data $SIG_{80,SAM1}$ is confirmed, the key file KF_{11} shown in Fig. 75B is read from the stack memory 200 and output to the encryptor/decryptor 173.

[0919] Then, the encryptor/decryptor 173 sequentially encrypts the key file KF_{11} by using the storage key data K_{STR}, media key data K_{MED}, and the purchaser key data K_{PIN} read from the storage unit 192 and outputs the same to the media SAM manager 197.

[0920] Step SV4: The media SAM manager 197 outputs the content file CF input from the SAM manager 190 and the key file KF_{11} input from the encryptor/decryptor 173 to the storage module 260 shown in Fig. 72.

[0921] Then, the storage module 260 writes the content file CF and the key file KF_{11} input from the media SAM manager 197 into the RAM region 251 of the RAM type storage media 250 shown in Fig. 72.

[0922] Note that, in the processing in the SAM 305_1, the flow of the processing in the AV apparatus 360_2 when determining the purchase mode of a ROM type storage medium having the not yet determined purchase mode of the content and the flow of the processing when reading the secure container 304 from a ROM type storage medium having the not yet determined purchase mode in the AV apparatus 360_3 and transferring this to the AV apparatus 360_2 and writing the same into the RAM type storage medium are the same as the case of the SAM 105_1 of the first embodiment except the point that the verification of the signature data using the secret key data of the service provider 310 is carried out and the point that the price tag data 312 is stored in the key file having the purchase mode determined.

[0923] Next, an explanation will be made of the overall operation of the EMD system 300 shown in Fig. 49.

[0924] Figure 78 and Fig. 79 are flowcharts of the overall operation of the EMD system 300.

[0925] Here, an explanation will be made by illustrating the case where the secure container 304 is trans-

mitted from the service provider 310 to the user home network 303 on-line.

[0926] Note that, as the prerequisite of the following processing, it is assumed that the content provider 301, service provider 310, and SAMs 305_1 to 305_4 have already been registered at the EMD service center 302.

[0927] Step S21: The EMD service center 302 transmits the certificate CER_{CP} of the public key data $K_{CP,P}$ of the content provider 301 together with its own signature data $SIG_{1,ESC}$ to the content provider 301.

[0928] Further, the EMD service center 302 transmits the certificate CER_{SP} of the public key data $K_{SP,P}$ the content provider 301 together with its own signature data $SIG_{61,ESC}$ to the service provider 310.

[0929] Further, the EMD service center 302 transmits six months' worth of the distribution key data KD_1 to KD_6 each having a term of validity of one month to the content provider 301 and transmits three months' worth of the distribution key data KD_1 to KD_3 to the SAMs 305_1 to 305_4 of the user home network 303.

[0930] Step S22: The content provider 301 transmits the right registration request module Mod_2 shown in Fig. 7A to the EMD service center 302.

[0931] Then, the EMD service center 302 registers and authorizes (certifies) the usage control policy data 106 and content key data Kc after the predetermined signature verification.

[0932] Step S23: The content provider 301 supplies the secure container 104 storing the data shown in Fig. 4A, Fig. 4B, and Fig. 4C to the service provider 310 after the processing for preparation of the signature data and the encryption processing using the distribution key data KD_1 to KD_3 of the corresponding period etc.

[0933] Step S24: The service provider 310 verifies the signature data $SIG_{1,ESC}$ shown in Fig. 4C and then verifies the signature data $SIG_{8,CP}$ and $SIG_{7,CP}$ shown in Figs. 4A and 4B by using the public key data $K_{CP,P}$ stored in the public key certificate data CER_{CP} to confirm if the secure container 104 was transmitted from a legitimate content provider 301.

[0934] Step S25: The service provider 310 generates the price tag data 312 and generates the secure container 304 shown in Fig. 53 storing the price tag data 312.

[0935] Step S26: The service provider 310 transmits the price tag registration request module Mod_{102} shown in Fig. 55 to the EMD service center 302.

[0936] Then, the EMD service center 302 registers and authorizes the price tag data 312 after the predetermined signature verification.

[0937] Step S27: The service provider 310 transmits the secure container 304 generated at step S25 on-line or off-line to the decryption module 905 of the network apparatus 360_1 shown in Fig. 63 in response to the request from for example the CA module 311 of the user home network 303.

[0938] Step S28: The CA module 311 generates the SP use purchase log data 309 and transmits this to the service provider 310 at the predetermined timing.

[0939] Step S29: Each of the SAMs 305_1 to 305_4, after verifying the signature data $SIG_{61,ESC}$ shown in Fig. 53D, verifies the signature data $SIG_{62,SP}$, $SIG_{63,SP}$, and $SIG_{64,SP}$ shown in Figs. 53A, 53B, and 53C by using the public key data $K_{SP,P}$ stored in the public key certificate data CER_{SP} to confirm if the secure container 304 is transmitted from a legitimate service provider 310.

[0940] Step S30: Each of the SAMs 305_1 to 305_4 decrypts the key file KF shown in Fig. 53B by using the distribution key data KD_1 to KD_3. Then, each of the SAMs 305_1 to 305_4, after verifying the signature data $SIG_{1,ESC}$ shown in Fig. 53B, verifies the signature data $SIG_{2,CP}$, $SIG_{3,CP}$, and $SIG_{4,CP}$ shown in Fig. 53B by using the public key data $K_{CP,P}$ stored in the public key certificate data CER_{CP} to confirm if the content data C, content key data Kc, and usage control policy data 106 were generated by a legitimate content provider 301.

[0941] Step S31: The user operates the purchase/usage mode determination controller 165 of Fig. 63 to determine the purchase and/or usage mode of the content.

[0942] Step S32: Based on the control signal S165 generated at step S31, the SAMs 305_1 to 305_4 generate the usage log data 308 of the secure container 304.

[0943] The usage log data 308 and the signature data $SIG_{205,SAM1}$ thereof are transmitted from the SAMs 305_1 to 305_4 to the EMD service center 302.

[0944] The EMD service center 302 determines (calculates) the charge content for each of the content provider 301 and the service provider 310 based on the usage log data 308 and generates the settlement claim data 152c and 152s based on the result thereof.

[0945] The EMD service center 302 transmits the settlement claim data 152c and 152s together with its own signature data to the settlement organization 91 via the payment gateway 90. By this, the money paid by the user of the user home network 303 to the settlement organization 91 is distributed to the owners of the content provider 301 and the service provider 310.

[0946] As explained above, the EMD system 300 distributes the secure container 104 of the format shown in Fig. 4 from the content provider 301 to the service provider 310 and distributes the secure container 304 storing the content file CF and key file KF in the secure container 104 as they are from the service provider 310 to the user home network 303 and performs the processing for the key file KF in the SAMs 305_1 to 305_4.

[0947] Also, the content key data Kc and usage control policy data 106 stored in the key file KF are encrypted by using the distribution key data KD_1 to KD_3 and decrypted in only the SAMs 305_1 to 305_4 holding the distribution key data KD_1 to KD_3. The SAMs 305_1 to 305_4 are modules having tamper resistance. The purchase mode and the usage mode of the content data C are determined based on the handling content of the content data C described in the usage control policy data 106.

[0948] Accordingly, according to the EMD system

300, the purchase and usage of the content data C in the user home network 303 can be reliably performed based on the content of the usage control policy data 106 generated by the related parties of the content provider 101 regardless of the processing in the service provider 310. Namely, according to the EMD system 300, it is possible to prevent the usage control policy data 106 from not being able to be managed by the service provider 310.

[0949] For this reason, according to the EMD system 300, even in a case where the content data C is distributed to the user home network 303 via a plurality of service providers 310 of different series, the right clearing for the related content data C in the user home network 303 can be performed based on the common usage control policy data 106 generated by the content provider 301.

[0950] Further, the EMD system 300 enables common right clearing of the content data C in the SAMs 305_1 to 305_4 both on-line and off-line by distributing the content data C from the content provider 301 to the user home network 103 by using the secure container 304 in both cases.

[0951] Further, the EMD system 300 enables use of common right clearing rules when purchasing, using, storing, and transferring the content data C in the network apparatus 360_1 and the AV apparatuses 360_2 to 360_4 in the user home network 303 by performing processing always based on the usage control policy data 106.

[0952] Further, according to the EMD system 300, since the EMD service center 302 has an authentication function, key data management function, and right clearing (profit distribution) function, the money paid by the user accompanied with the usage of the content is reliably distributed to the owners of the content provider 301 and the EMD service center 302 according to the ratio determined in advance.

[0953] Further, according to the EMD system 300, the usage control policy data 106 for the same content file CF supplied by the same content provider 301 is supplied as it is to the SAMs 305_1 to 305_4 regardless of the service mode of the service provider 310. Accordingly, the SAMs 305_1 to 305_4 can use the content file according to the intention of the content provider 301 based on the usage control policy data 106.

[0954] Namely, according to the EMD system 300, when the service using the content and the user use the content, the rights and profit of the owner of the content provider 301 can be reliably protected by technical means without depending on an inspection organization 725 as in the conventional case.

First Modification of Second Embodiment

[0955] Figure 80 is a view of the configuration of an EMD system 300a using two service providers according to a first modification of the second embodiment.

[0956] In Fig. 80, components given the same references as those of Fig. 49 are the same as the components having the same references explained in the second embodiment.

[0957] As shown in Fig. 80, the EMD system 300a supplies the same secure container 104 from the content provider 301 to the service providers 310a and 310b.

[0958] The service provider 310a provides the service of providing for example a drama program as content. This service generates a secure container 304a storing the content data C related to the related drama program and price tag data 312a uniquely generated for the related content data C and distributes this to the network apparatus 360_1.

[0959] Further, the service provider 310b provides for example a karaoke service. This service generates a secure container 304b storing the content data C related to the related karaoke service and price tag data 312b uniquely generated for the related content data C and distributes this to the network apparatus 3601.

[0960] Here, the formats of the secure containers 304a and 304b are the same as that of the secure container 304 explained by using Fig. 53.

[0961] A network apparatus $360a_1$ is provided with CA modules 311a and 311b corresponding to the service providers 310a and 310b.

[0962] The CA modules 311a and 311b receive the distribution of the secure containers 304a and 304b from the service providers 310a and 310b in response to their own requests.

[0963] Next, the CA modules 311a and 311b generate SP use purchase log data 309a and 309b in accordance with the distributed secure containers 304a and 304b and transmit them to the service providers 310a and 310b.

[0964] Further, the CA modules 311a and 311b decrypt the secure containers 304a and 304b by the session key data K_{SES} and then output the same to the SAMs 305_1 to 305_4.

[0965] Next, the SAMs 305_1 to 305_4 decrypt the key files KF in the secure containers 304a and 304b by using the common distribution key data KD_1 to KD_3, perform the processing concerning the purchase and/or usage of the content in accordance with the operation from the user based on the common usage control policy data 106, and generate the usage log data 308 in accordance with that .

[0966] Then, the usage log data 308 is transmitted from the SAMs 305_1 to 305_4 to the EMD service center 302.

[0967] The EMD service center 302, based on the usage log data 308, determines (calculates) the charge content for each of the content provider 301 and the service providers 310a and 310b and generates the settlement claim data 152c, 152sa, and 152sb corresponding to them based on the results thereof.

[0968] The EMD service center 302 transmits the set-

tlement claim data 152c, 152sa, and 152sb to the settlement organization 91 via the payment gateway 90. By this, the money paid by the user of the user home network 303 to the settlement organization 91 is distributed to the owners of the content provider 301 and the service providers 310a and 310b.

[0969] As mentioned above, according to the EMD system 300b, when supplying the same content file CF to the service providers 310a and 310b, the usage control policy data 106 for the related content file CF is encrypted by the distribution key data KD_1 to KD_6 and supplied to the service providers 310a and 310b, and the service providers 310a and 310b distribute the secure containers 304a and 304b storing the encrypted usage control policy data 106 as it is to the user home network. For this reason, the SAMs 305_1 to 305_4 in the user home network can perform right clearing based on the common usage control policy data 106 no matter from which of the service providers 310a or 310b the content file CF is distributed.

[0970] Note that, in the first modification, the case where two service providers were used was illustrated, but in the present invention, any number of the service provider may be used.

Second Modification of Second Embodiment

[0971] Figure 81 is a view of the configuration of an EMD system 300b using a plurality of content providers according to a second modification of the second embodiment.

[0972] In Fig. 81, components given the same references as those of Fig. 49 are the same as the components having the same references explained in the second embodiment.

[0973] As shown in Fig. 81, the EMD system 300b supplies the secure containers 104a and 104b from content providers 301a and 301b to the service provider 310.

[0974] The service provider 310 provides the service by using the content supplied by for example the content providers 301a and 301b, generates the price tag data 312a for the secure container 104a and the price tag data 312b for the secure container 104b, and generates a secure container 304c storing them.

[0975] As shown in Fig. 81, the secure container 304c stores the content data CFa, CFb, key files KFa and KFb, price tag data 312a and 312b, and signature data based on the secret key data $K_{CP,S}$ of the service provider 310 for each of them.

[0976] The secure container 304c is received at the CA module 311 of the network apparatus 3601 of the user home network 303 and then processed at the SAMs 305_1 to 305_4.

[0977] The SAMs 305_1 to 305_4 decrypt the key file KFa by using the distribution key data KDa_1 to KDa_3, perform the processing concerning the purchase and/or usage in accordance with the operation from the user for the content file CFa based on the usage control policy data 106a, and describe the log thereof in the usage log data 308.

[0978] Further, the SAMs 305_1 to 305_4 decrypt the key file KFb by using distribution key data KDb_1 to KDb_3, perform the processing concerning the purchase and/or usage in accordance with the operation from the user for the content file CFb based on the usage control policy data 106b, and describe the log thereof in the usage log data 308.

[0979] Then, the usage log data 308 is transmitted from the SAMs 305_1 to 305_4 to the EMD service center 302.

[0980] The EMD service center 302 determines (calculates) the charge content for each of the content providers 301a and 301b and the service provider 310 based on the usage log data 308 and generates settlement claim data 152ca, 152cb, and 152s corresponding to them based on the results thereof.

[0981] The EMD service center 302 transmits the settlement claim data 152ca, 152cb, and 152s via the payment gateway 90 to the settlement organization 91 and distributes the money paid by the user of the user home network 303 to the settlement organization 91 to the owners of the content providers 301a and 301b and the service provider 310 by this.

[0982] As mentioned above, according to the EMD system 300b, as the usage control policy data 106a and 106b of the content files CFa and CFb stored in the secure container 304, those generated by the content providers 301a and 301b are used as they are, therefore, the SAMs 305_1 to 305_4 reliably carry out the right clearing for the content files CFa and CFb based on the usage control policy data 106a and 106b according to the intention of the content providers 301a and 301b.

[0983] Note that, in the second modification shown in Fig. 81, the case where two content providers were used was illustrated, but any number of the content providers may be used.

[0984] Further, there may be a plurality of both of the content providers and service providers.

Third Modification of Second Embodiment

[0985] Figure 82 is a view of the configuration of the EMD system according to a third modification of the second embodiment.

[0986] In the second embodiment, the case where the EMD service center 302 performed the settlement of the content provider 301 and the service provider 310 with respect to the settlement organization 91 was illustrated, but in the present invention, for example, as shown in Fig. 82, it is also possible that the settlement claim data 152c for the content provider 301 and the settlement claim data 152s for the service provider 310 be generated based on the usage log data 308 in the EMD service center 302 and that they be transmitted to the content provider 301 and the service provider 310.

[0987] In this case, the content provider 301 performs the settlement at a settlement organization 91a via a payment gateway 90a by using the settlement claim data 152c. Further, the service provider 310 performs the settlement at a settlement organization 91b via a payment gateway 90b by using the settlement claim data 152s.

Fourth Modification of Second Embodiment

[0988] Figure 83 is a view of the configuration of the EMD system according to a fourth modification of the second embodiment.

[0989] In the second embodiment, the case where the service provider 310 did not have a charging function as in for example the current Internet was illustrated, but where the service provider 310 has a charging function as in the current digital broadcasting, the CA module 311 generates a usage log data 308s with respect to the service of the service provider 310 concerning the secure container 304 and transmits it to the service provider 310.

[0990] Then, the service provider 310 performs the charge processing based on the usage log data 308s to generate the settlement claim data 152s and performs the settlement at the settlement organization 91b via the payment gateway 90b by using this.

[0991] On the other hand, the SAMs 305_1 to 305_4 generate usage log data 308c with respect to the right clearing of the content provider 301 concerning the secure container 304 and transmit them to the EMD service center 302.

[0992] The EMD service center 302 generates the settlement claim data 152c based on the usage log data 308c and transmits this to the content provider 301.

[0993] The content provider 301 performs the settlement at the settlement organization 91a via the payment gateway 90a by using the settlement claim data 152c.

Fifth Modification of Second Embodiment

[0994] In the embodiment, as shown in Fig. 49, the case where the user preference filter data 903 was generated based on the usage log data 308 received from the SAM 305_1 etc. in the user preference filter creator 901 of the EMD service center 302 was illustrated, but it is also possible that for example the usage control status data 166 generated at the usage monitor 186 such as the SAM 305_1 shown in Fig. 67 be transmitted to the EMD service center 302 in real-time and that the user preference filter data 903 be generated based on the usage control status data 166 in the SP use purchase log data 309.

Sixth Modification of Second Embodiment

[0995] The content provider 301, the service provider 310, and the SAMs 305_1 to 305_4 can register their secret key data $K_{CP,S}$, $K_{SP,S}$, and $K_{SAM1,S}$ to $K_{SAM4,S}$ in the EMD service center 302 too other than their public key data $K_{CP,P}$, $K_{SP,P}$, and $K_{SAM1,P}$ to $K_{SAM4,P}$.

[0996] By doing this, it becomes possible for the EMD service center 302 to tap communication concerned in the communication between the content provider 301 and the service provider 310, the communication between the service provider 310 and the SAMs 305_1 to 305_4, and the communication among the SAMs 305_1 to 305_4 in the user home network 303 by using the secret key data $K_{CP,S}$, $K_{SP,S}$, and $K_{SAM1,S}$ to $K_{SAM4,S}$ in response to demands from the nation or the police organization at the time of an emergency.

[0997] Further, it is also possible that the secret key data $K_{SAM1,S}$ to $K_{SAM4,S}$ be generated for the SAMs 305_1 to 305_4 by the EMD service center 302 at the time of shipping and that they be stored in the SAMs 305_1 to 305_4 and, at the same time, held (registered) by the EMD service center 302.

Seventh Modification of Second Embodiment

[0998] In the above embodiment, the case where public key certificate data CER_{CP}, CER_{SP}, and CER_{SAM1} to CER_{SAM4} were acquired from the EMD service center 302 in advance when the content provider 301, service provider 310, and SAMs 305_1 to 305_4 communicated with respect to each other and were transmitted to the destination of communication by the in-band method was illustrated, but in the present invention, various modes can be employed as the mode of transmission of public key certificate data to the destination of communication.

[0999] For example, it is also possible that the public key certificate data CER_{CP}, CER_{SP}, and CER_{SAM1} to CER_{SAM4} be acquired from the EMD service center 302 in advance when the content provider 301, service provider 310, and the SAM 305_1 to 305_4 communicate with respect to each other and be transmitted to the destination of communication by the in-band method preceding the related communication.

[1000] Further, it is also possible for the content provider 301, the service provider 310, and the SAM 305_1 to 305_4 to acquire the public key certificate data CER_{CP}, CER_{SP} and CER_{SAM1} to CER_{SAM4} from the EMD service center 302 at the time of communication.

[1001] Figure 84 is a view for explaining the mode of the route of acquiring the public key certificate data.

[1002] Note that, in Fig. 84, components given the same references as those of Fig. 49 are the same as the components having the same references. Further, a user home network 303a is the same as the user home network 303 mentioned before. In a user home network 303b, SAMs 305_{11} to 305_{14} are connected via a bus 191, that is, an IEEE 1394 serial bus.

[1003] When the content provider 301 acquires the public key certificate data CER_{SP} of the service provider 310, there are for example a case where the public key

certificate data CER_{SP} is transmitted from the service provider 310 to the content provider 301 preceding the communication ((3) in Fig. 84) and a case where the content provider 301 orders the public key certificate data CER_{SP} from the EMD service center 302 ((1) in Fig. 84).

[1004] Further, when the service provider 310 acquires the public key certificate data CER_{CP} of the content provider 301, there are for example a case where the public key certificate data CER_{CP} is transmitted from the content provider 301 to the service provider 310 preceding the communication ((2) in Fig. 84) and a case where the service provider 310 orders the public key certificate data CER_{CP} from the EMD service center 302 ((4) in Fig. 84).

[1005] Further, when the service provider 310 acquires the public key certificate data CER_{SAM1} to CER_{SAM4} of the SAMs 305_1 to 305_4, there are for example a case where the public key certificate data CER_{SAM1} to CER_{SAM4} are transmitted from the SAMs 305_1 to 305_4 to the service provider 310 preceding the communication ((6) in Fig. 84) and a case where the service provider 310 orders the public key certificate data CER_{SAM1} to CER_{SAM4} from the EMD service center 302 ((4) in Fig. 84).

[1006] Further, when the SAMs 305_1 to 305_4 acquire the public key certificate data CER_{SP} of the service provider 310, there are for example a case where the public key certificate data CER_{SP} is transmitted from the service provider 310 to the SAMs 305_1 to 305_4 preceding the communication ((5) in Fig. 84) and a case where the SAMs 3051 to 305_4 order the public key certificate data CER_{SP} from the EMD service center 302 ((7) in Fig. 84, etc.).

[1007] Further, when the SAM 305_1 acquires the public key certificate data CER_{SAM2} of the SAM 305_2, there are for example a case where the public key certificate data CER_{SAM2} is transmitted from the SAM 305_2 to the SAM 305_1 preceding the communication ((8) in Fig. 84) and a case where the SAM 305_1 orders the public key certificate data CER_{SAM2} from the EMD service center 302 ((7) in Fig. 84, etc.).

[1008] Further, when the SAM 305_2 acquires the public key certificate data CER_{SAM1} of the SAM 305_1, there are for example a case where the public key certificate data CER_{SAM1} is transmitted from the SAM 305_1 to the SAM 305_2 preceding the communication ((9) in Fig. 84), a case where the SAM 305_2 orders the public key certificate data CER_{SAM1} from the EMD service center 302 by itself, and a case where the SAM 305_2 orders the public key certificate data CER_{SAM1} via the network apparatus with the SAM 305_1 mounted therein ((7), (8) in Fig. 84).

[1009] Further, when the SAM 305_4 acquires the public key certificate data CER_{SAM13} of the SAM 305_{13}, there are for example a case where the public key certificate data CER_{SAM13} is transmitted from the SAM 305_{13} to the SAM 305_4 preceding the communication ((12) in Fig. 84), a case where the SAM 305_4 orders the public key certificate data CER_{SAM13} from the EMD service center 302 by itself ((10) in Fig. 84), and a case where the SAM 305_4 orders the public key certificate data CER_{SAM13} via the network apparatus in the user home network 303b.

[1010] Further, when the SAM 305_{13} acquires the public key certificate data CER_{SAM4} of the SAM 305_4, there are for example a case where the public key certificate data CER_{SAM4} is transmitted from the SAM 305_4 to the SAM 305_{13} preceding the communication ((11) in Fig. 84), a case where the SAM 305_{13} orders the public key certificate data CER_{SAM4} from the EMD service center 302 by itself ((13) in Fig. 84), and a case where the SAM 305_{13} orders the public key certificate data CER_{SAM4} via the network apparatus in the user home network 303b.

Handling of Public Key Certificate Revocation List (Data) in Second Embodiment

[1011] In the second embodiment, in order to prevent a content provider 301, a service provider 310, and SAMs 305_1 to 305_4 used for an illegal action etc. from communicating with another apparatus in the EMD service center 302, the public key certificate revocation list for invalidating the public key certificate data of the apparatus used for the related illegal action is generated. Then, the related public key certificate revocation list CRL is transmitted to the content provider 301, service provider 310, and SAMs 305_1 to 305_4.

[1012] Note that, it is also possible that the public key certificate revocation list CRL be generated in for example the content provider 301, the service provider 310, and the SAMs 305_1 to 305_4 other than the EMD service center 302.

[1013] First, an explanation will be made of the case where the EMD service center 302 invalidates the public key certificate data CER_{CP} of the content provider 301.

[1014] As shown in Fig. 85, the EMD service center 302 transmits a public key certificate revocation list CRL_1 indicating the invalidation of the public key certificate data CER_{CP} to the service provider 310 ((1) in Fig. 85). When verifying the signature data input from the content provider 301, the service provider 310 decides the validity of the public key certificate data CER_{CP} by referring to the public key certificate revocation list CRL_1, verifies the signature using the public key data $K_{CP,P}$ when it decides that it is valid, and invalidates the data from the content provider 301 without verifying the signature when it decides that it is invalid. Note that, it is also possible not to invalidate the data, but reject the communication.

[1015] Further, the EMD service center 302 transmits the public key certificate revocation list CRL_1 to for example the SAM 305_1 in the user home network 303 by utilizing distribution resources of the service provider 310 by either one of the broadcast type or on-demand

type ((1), (2) in Fig. 85). When verifying the signature data of the content provider 301 stored in the secure container input from the service provider 310, the SAM 305_1 decides the validity of the public key certificate data CER_{CP} by referring to the public key certificate revocation list CRL_1, verifies the signature using the public key data $K_{CP,P}$ when it decides it is valid, and invalidates the related secure container without verifying the signature when it decides it is invalid.

[1016] Note that, it is also possible for the EMD service center 302 to directly transmit the public key certificate revocation list CRL_1 to the SAM 305_1 via the network apparatus in the user home network 303 ((3) in Fig. 85).

[1017] Next, an explanation will be made of the case where the EMD service center 302 invalidates the public key certificate data CER_{SP} of the service provider 310.

[1018] As shown in Fig. 86, the EMD service center 302 transmits a public key certificate revocation list CRL_2 indicating the invalidation of the public key certificate data CER_{SP} to the content provider 301 ((1) in Fig. 86). When verifying the signature data input from the service provider 310, the content provider 301 decides the validity of the public key certificate data CER_{SP} by referring to the public key certificate revocation list CRL_2, verifies the signature using the public key data $K_{SP,P}$ when it decides it is valid, and invalidates the data from the service provider 310 without verifying the related signature when it decides it is invalid.

[1019] Further, the EMD service center 302 transmits the public key certificate revocation list CRL_2 to for example the SAM 305_1 in the user home network 303 by utilizing the distribution resources of the service provider 310 by either the broadcast type or on-demand type ((2) in Fig. 86). When verifying the signature data of the content provider 301 stored in the secure container input from the service provider 310, the SAM 305_1 decides the validity of the public key certificate data CER_{SP} by referring to the public key certificate revocation list CRL_2, verifies the signature using the public key data $K_{SP,P}$ when it decides it is valid, and invalidates the related secure container without verifying the signature when it decides it is invalid.

[1020] In this case, in the service provider 310, the module for transferring the public key certificate revocation list CRL_2 must have tamper resistance. Further, in the service provider 310, the public key certificate revocation list CRL_2 must be stored in a region where tampering by related parties of the service provider 310 is difficult.

[1021] Note that, it is also possible for the EMD service center 302 to directly transmit the public key certificate revocation list CRL_2 to the SAM 305_1 via the network apparatus in the user home network 303 ((3) in Fig. 86).

[1022] Next, an explanation will be made of a case where the EMD service center 302 invalidates for example the public key certificate data CER_{SAM2} of the SAM 305_2.

[1023] As shown in Fig. 87, the EMD service center 302 transmits a public key certificate revocation list CRL_3 indicating the invalidation of the public key certificate data CER_{SAM2} to the content provider 301 ((1) in Fig. 87). The content provider 301 transmits the public key certificate revocation list CRL_3 to the service provider 310. The service provider 310 transmits the public key certificate revocation list CRL_3 to for example the SAM 305_1 in the user home network 303 by utilizing its own distribution resources by either the broadcast type or on-demand type ((1) in Fig. 87). When verifying the signature data of the SAM 305_2 added to the data input from the SAM 305_2, the SAM 305_1 decides the validity of the public key certificate data CER_{SAM2} by referring to the public key certificate revocation list CRL_3, verifies the signature using the public key data $K_{SAM2,P}$ when it decides it is valid, and invalidates the related data without verifying the signature when it decides it is invalid.

[1024] In this case, in the service provider 310, the module for transferring the public key certificate revocation list CRL_3 must have tamper resistance. Further, in the service provider 310, the public key certificate revocation list CRL_3 must be stored in a region where tampering by related parties of the service provider 310 is difficult.

[1025] It is also possible for the EMD service center 302 to transmit the public key certificate revocation list CRL_3 to the SAM 305_1 via the service provider 310 ((1), (2) in Fig. 87).

[1026] Note that, it is also possible for the EMD service center 302 to directly transmit the public key certificate revocation list CRL_3 to the SAM 305_1 via the network apparatus in the user home network 303 ((3) in Fig. 87).

[1027] Further, the EMD service center 302 generates and stores the public key certificate revocation list CRL_3 indicating the invalidation of for example the public key certificate data CER_{SAM2} of the SAM 305_2.

[1028] Further, the user home network 303 generates a SAM registration list SRL of the SAMs connected to the bus 191 and transmits this to the EMD service center 302 ((1) in Fig. 88).

[1029] The EMD service center 302 identifies the SAMs (for example SAM 305_2) for which invalidation is indicated by the public key certificate revocation list CRL_3 among the SAMs 305_1 to 305_4 indicated in the SAM registration list, sets revocation flags corresponding to the related SAMs in the SAM registration list SRL so as to indicate the invalidity, and thereby generates a new SAM registration list SRL.

[1030] Next, the EMD service center 302 transmits the related generated SAM registration list SRL to the SAM 305_1 ((1) in Fig. 88).

[1031] The SAM 305_1 determines the existence of the verification of the signature data and whether or not the communication is permitted by referring to the revocation flags of the SAM registration list SRL when commu-

nicating with another SAM.

[1032] Further, the EMD service center 302 generates the public key certificate revocation list CRL_3 and transmits this to the content provider 301 ((2) in Fig. 88).

[1033] The content provider 301 transmits the public key certificate revocation list CRL_3 to the service provider 310 ((2) in Fig. 88).

[1034] Next, the service provider 310 transmits the public key certificate revocation list CRL_3 to the SAM 305_1 by either the broadcast type or on-demand type by utilizing its own distribution resources ((2) in Fig. 88).

[1035] The SAM 305_1 identifies the SAM (for example SAM 305_2) for which invalidation is indicated by the public key certificate revocation list CRL_3 among the SAMs 305_1 to 305_4 indicated in the SAM registration list generated by itself and sets revocation flags corresponding to the related SAMs in the SAM registration list SRL so as to indicate the invalidity.

[1036] After that, the SAM 305_1 determines the existence of the verification of the signature data and whether or not communication is permitted by referring to the revocation flags of the related SAM registration list SRL when communicating with another SAM.

[1037] Further, the EMD service center 302 generates the public key certificate revocation list CRL_3 and transmits this to the service provider 310 ((3) in Fig. 88).

[1038] Next, the service provider 310 transmits the public key certificate revocation list CRL_3 to the SAM 305_1 by either one the broadcast type or on-demand type by utilizing its own distribution resources ((3) in Fig. 88).

[1039] The SAM 305_1 specifies the SAMs (for example SAM 305_2) for which invalidation is indicated by the public key certificate revocation list CRL_3 among the SAMs 305_1 to 305_4 indicated in the SAM registration list generated by itself and sets revocation flags corresponding to the related SAMs in the SAM registration list SRL so as to indicate the invalidity.

[1040] After that, the SAM 305_1 determines the existence of the verification of the signature data and whether or not communication is permitted by referring to the revocation flags of the related SAM registration list SRL when communicating with another SAM.

Role Etc. of EMD Service Center 302

[1041] Figure 89 is a view of the configuration of the EMD system when the functions of the EMD service center (clearing house) 302 shown in Fig. 49 are divided between a right management clearing house 950 and an electronic settlement clearing house 951.

[1042] In the related EMD system, in the electronic settlement clearing house 951 performs the settlement processing (profit distribution processing) based on the usage log data 308 from the SAMs of the user home networks 303a and 303b, generates the settlement claim data of the content provider 301 and the service provider 310, and performs settlement at the settlement organization 91 via the payment gateway 90.

[1043] Further, the right management clearing house 950 generates the settlement reports of the content provider 301 and the service provider 310 in accordance with the settlement notification from the electronic settlement clearing house 951 and transmits them to the content provider 301 and the service provider 310.

[1044] Further, it performs the registration (authorization) etc. of the usage control policy data 106 and the content key data Kc of the content provider 301.

[1045] Note that, as shown in Fig. 90, when the right management clearing house 950 and the electronic settlement clearing house 951 are accommodated in a single apparatus, the EMD service center 302 shown in Fig. 49 is formed.

[1046] Further, in the present invention, for example, as shown in Fig. 91, it is also possible to provide the functions of a right management clearing house 960 in the EMD service center 302, perform the registration etc. of the usage control policy data 106 in the right management clearing house 960 and, at the same time, generate the settlement claim data of the service provider 310 based on the usage log data 308 from the SAMs and transmit this to the service provider 310. In this case, the service provider 310 utilizes its own charge system as an electronic settlement clearing house 961 and performs the settlement based on the settlement claim data from the right management clearing house 960.

[1047] Further, in the present invention, for example as shown in Fig. 92, it is also possible to provide the function of a right management clearing house 970 in the EMD service center 302, perform the registration etc. of the usage control policy data 106 in the right management clearing house 970 and, at the same time, generate the settlement claim data of the content provider 301 based on the usage log data 308 from the SAM and transmit this to the content provider 301. In this case, the content provider 301 utilizes its own charge system as an electronic settlement clearing house 971 and performs the settlement based on the settlement claim data from the right management clearing house 970.

Eighth Modification of Second Embodiment

[1048] In the second embodiment, the case where the secure container 104 of the format shown in Fig. 4 was provided from the content provider 301 to the service provider 310 and the secure container 304 of the format shown in Fig. 53 was distributed from the service provider 310 to the user home network 303 in the EMD system 300 shown in Fig. 49 was illustrated.

[1049] Namely, in the second embodiment, as shown in Fig. 4 and Fig. 53, the case of storing a single content file CF and a single key file KF corresponding to the related content file CF in the secure container 104 and the secure container 304 was illustrated.

[1050] In the present invention, it is also possible to

store a plurality of content files CF and a plurality of key files KF corresponding to the related plurality of content files CF in the secure container 104 and the secure container 304.

[1051] Figure 93 is a view for explaining the format of the secure container 104a provided from the content provider 301 to the service provider 310 shown in Fig. 49 in the present modification.

[1052] As shown in Fig. 93, the secure container 104a stores the content files CF_{101}, CF_{102}, and CF_{103}, the key files KF_{101}, KF_{102}, and KF_{103}, the public key certificate data CER_{CP}, the signature data $SIG_{1,ESC}$, and the signature data $SIG_{C250,CP}$.

[1053] Here, the signature data $SIG_{C250,CP}$ is generated by the content provider 301 taking the hush values with respect to all of the content files CF_{101}, CF_{102}, and CF_{103}, the key files KF_{101}, KF_{102}, and KF_{103}, the public key certificate data CER_{CP}, and the signature data $SIG_{1,ESC}$ using the secret key data $K_{CP,S}$ of the content provider 301.

[1054] The content file CF_{101} stores a header, link data LD_1, meta-data $Meta_1$, content data C_1, and an A/V decompression software $Soft_1$.

[1055] Here, the content data C_1 and the A/V decompression software $Soft_1$ is encrypted by using the content key data Kc_1 mentioned above, while the meta-data $Meta_1$ is encrypted by using the content key data Kc_1 according to need.

[1056] Further, the content data C_1 is compressed by for example the ATRAC3 method. The A/V decompression software $Soft_1$ is the software for the decompression of the ATRAC3 method.

[1057] Further, the link data LD_1 indicates the link to the key file KF_{101}.

[1058] The content file CF_{102} stores the header, link data LD_2, meta-data $Meta_2$, content data C_2, and an A/V decompression software $Soft_2$ are stored.

[1059] Here, the content data C_2 and the A/V decompression software $Soft_2$ are encrypted by using the content key data Kc_2 mentioned above, while the meta-data $Meta_2$ is encrypted by using the content key data Kc_2 according to need.

[1060] Further, the content data C_2 is compressed by for example the MPEG2 method. The A/V decompression software $Soft_2$ is the software for the decompression of the MPEG2 method.

[1061] Further, the link data LD_2 indicates the link to the key file KF_{102}.

[1062] The content file CF_{103} stores a header, link data LD_3, meta-data $Meta_3$, content data C_2, and an A/V decompression software $Soft_3$.

[1063] Here, the content data C_3 and the A/V decompression software $Soft_3$ are encrypted by using the content key data Kc_3 mentioned above, while the meta-data $Meta_3$ is encrypted by using the content key data Kc_3 according to need. Further, the content data C_3 is compressed by for example the JPEG method. The A/V decompression software $Soft_3$ is software for the decompression of the JPEG method.

[1064] Further, the link data LD_3 indicates the link to the key file KF_{103}.

[1065] The key file KF_{101} stores a header, content key data Kc_1 encrypted by using the distribution key data KD_1 to KD_3, usage control policy data 106_1, SAM program download container SDC_1, and signature certificate module Mod_{200}.

[1066] Here, the signature certificate module Mod_{200}, as shown in Fig. 94A, stores the signature data $SIG_{211,CP}$, $SIG_{212,CP}$, and $SIG_{213,CP}$ generated by taking the hush values of the content data C_1, content key data Kc_1, and the usage control policy data 106_1 and using the secret key data $K_{CP,S}$ of the content provider 301, the public key certificate data CER_{CP} of the public key data $K_{CP,P}$, and the signature data $SIG_{1,ESC}$ of the EMD service center 302 with respect to the related public key certificate data CER_{CP}.

[1067] The key file KF_{102} stores a header, content key data Kc_2 encrypted by using the distribution key data KD_1 to KD_3, usage control policy data 106_2, SAM program download container SDC_2, and a signature certificate module Mod_{201}.

[1068] Here, the signature certificate module Mod_{201}, as shown in Fig. 94B, stores the signature data $SIG_{221,CP}$, $SIG_{222,CP}$, and $SIG_{223,CP}$ generated by taking the hush values of the content data C_2, content key data Kc_2, and the usage control policy data 106_2 and using the secret key data $K_{CP,S}$ of the content provider 301, public key certificate data CER_{CP}, and signature data $SIG_{1,ESC}$ with respect to the related public key certificate data CER_{CP}.

[1069] The key file KF_{103} stores a header, content key data Kc_3 encrypted by using the distribution key data KD_1 to KD_3, usage control policy data 106_3, a SAM program download container SDC_3, and a signature certificate module Mod_{202}.

[1070] Here, the signature certificate module Mod_{202}, as shown in Fig. 94C, stores the signature data $SIG_{231,CP}$, $SIG_{232,CP}$, and $SIG_{233,CP}$ generated by taking the hush values of the content data C_3, content key data Kc_3, and usage control policy data 106_3 and using the secret key data $K_{CP,S}$ of the content provider 301, public key certificate data CER_{CP}, and signature data $SIG_{1,ESC}$ with respect to the related public key certificate data CER_{CP}.

[1071] When receiving the distribution of the secure container 104a shown in Fig. 93, the service provider 310 confirms the legitimacy of the signature data $SIG_{C250,CP}$ by using the public key data $K_{CP,P}$ stored in the public key certificate data CER_{CP} after confirming the legitimacy of the related public key certificate data CER_{CP} by using the public key data $K_{ESC,P}$ of the EMD service center 302.

[1072] Then, when confirming the legitimacy of the signature data $SIG_{C250,CP}$, as shown in Fig. 95, the service provider 310 generates the secure container 304a storing the content files CF_{101}, CF_{102}, and CF_{103} and

the key files KF_{101}, KF_{102}, and KF_{103} obtained from the secure container 104a, public key certificate data CER_{SP} of the service provider 310, signature data $SIG_{61,ESC}$, price tag data 312_1, 312_2, and 312_3, and a signature data $SIG_{260,SP}$.

[1073] Here, the price tag data 312_1, 312_2, and 312_3 indicate the sale prices of the content data C_1, C_2, and C_3.

[1074] Further, the signature data $SIG_{260,SP}$ is generated by taking the hush value with respect to all of the content files CF_{101}, CF_{102}, and CF_{103}, key files KF_{101}, KF_{102}, and KF_{103}, public key certificate data CER_{SP}, signature data $SIG_{61,ESC}$, and the price tag data 312_1, 312_2, and 312_3 and by using the secret key data $K_{SP,S}$ of the service provider 310.

[1075] The service provider 310 distributes the secure container 304a shown in Fig. 95 to the user home network 303.

[1076] In the user home network 303, the SAMs 305_1 to 305_4 confirm the legitimacy of the signature data $SIG_{61,ESC}$ stored in the secure container 304a, then confirm the legitimacy of the signature data $SIG_{260,SP}$ by using the public key data $K_{SP,KP}$ stored in the public key certificate data CER_{SP}.

[1077] Thereafter, the SAMs 305_1 to 305_4 perform the right clearing for the content data C_{101}, C_{102}, and C_{103} in accordance with the link statuses indicated in the links LD_1, LD_2, and LD_3 based on the key files KF_{101}, KF_{102}, and KF_{103}.

[1078] Note that, in the eighth modification, the case where the signature data $SIG_{C250,CP}$ with respect to all of the content files CF_{101}, CF_{102}, and CF_{103}, key files KF_{101}, KF_{102}, and KF_{103}, public key certificate data CER_{CP}, and signature data $SIG_{1,ESC}$ was generated in the content provider 301 as shown in Fig. 93 was illustrated, but it. is also possible to generate the signature data for each of for example the content files CF_{101}, CF_{102}, and CF_{103} and the key files KF_{101}, KF_{102}, and KF_{103} and store this in the secure container 104a.

[1079] Further, in the eighth modification, the case where the signature data $SIG_{260,CP}$ with respect to all of the content files CF_{101}, CF_{102}, and CF_{103}, key files KF_{101}, KF_{102}, and KF_{103}, public key certificate data CER_{SP}, signature data $SIG_{61,ESC}$, and price tag data 312_1, 312_2, and 312_3 was generated in the service provider 310 as shown in Fig. 95 was illustrated, but it is also possible to generate the signature data for each of them and store them in the secure container 304a.

[1080] Further, in the eighth modification, the case where the secure container 304 stored a plurality of content files CF_{101}, CF_{102}, and CF_{103} provided from the single service provider 310 in the single secure container 304a and distributed it to the user home network 303 was illustrated, but it is also possible to distribute a plurality of content files CF provided from a plurality of content providers 301a and 301b in the single secure container and distribute the same to the user home network 303 as shown in Fig. 81.

[1081] Note that, the format shown in Fig. 93 can be similarly applied to also the case where the secure container 104 is transmitted from the content provider 101 to the user home network 103 shown in Fig. 1 in the first embodiment.

[1082] Further, in the above embodiment, the case where the settlement processing was carried out based on the usage log data input from the SAM in the EMD service center was illustrated, but it is also possible to transmit the usage control status data from a SAM to the EMD service center whenever the purchase mode of the content is determined in the SAM and perform the settlement processing by using the received usage control status data in the EMD service center.

[1083] Below, the concept of the content file CF and the key file KF etc. generated in the content provider 101 will be summarized.

[1084] When the content provider 101 provides content by using the Internet, as shown in Fig. 96, a content file CF containing a header, content ID, encrypted content data C using the content key data Kc, and signature data is generated as shown in Fig. 96. After the usage control policy data indicating the handling of the related content data C and the content key data Kc are encrypted by the distribution key data of the predetermined reliable managers, that is, the EMD service centers 102 and 302, they are stored in the key file KF. Further, the key file KF stores a header and the content ID and, according to need, the meta-data and the signature data.

[1085] Then, the content file CF and key file KF are provided directly from the content provider 101 to the user home networks 103 and 303 or provided from the content provider 101 to the user home networks 103 and 303 via the service provider 310.

[1086] Further, when the content provider 101 provides the content by using the Internet, as shown in Fig. 97, it is possible even if the content key data Kc is not stored in the key file KF, but the content key data Kc encrypted by the distribution key data of the predetermined reliable managers, that is, the EMD service centers 102 and 302, are provided from the EMD service centers 102 and 302 to the user home networks 103 and 303.

[1087] Further, when the content provider 101 provides the content by using a digital broadcast, for example, as shown in Fig. 98, it provides the content data C encrypted by using the content key data Kc and the signature data from the content provider 101 to the user home networks 103 and 303 directly or via the service provider 310. In this case, the key data blocks corresponding to the key file KF shown in Fig. 97 are provided from the content provider 101 to the user home networks 103 and 303 directly or via the service provider 310.

[1088] Further, in this case, for example, as shown in Fig. 99, it is also possible to provide the content key data Kc encrypted by the distribution key data of the EMD service centers 102 and 302 as the predetermined reliable managers from the EMD service centers 102 and

302 to the user home networks 103 and 303.

CAPABILITY OF UTILIZATION IN INDUSTRY

[1089] As explained above, according to the present invention, the profit of related parties of the data providing apparatus is suitably protected.

[1090] Also, according to the present invention, the illicit tampering with the usage control policy data etc. can be suitably avoided.

[1091] Further, according to the present invention, the load of the inspection for protecting the profit of the related parties of the data providing apparatus can be reduced.

Claims

1. A data providing system for distributing content data from a data providing apparatus to a data processing apparatus, wherein

   said data providing apparatus distributes a module storing the content data encrypted by using content key data, encrypted content key data, and an encrypted usage control policy data indicating handling of said content data to said data processing apparatus and
   said data processing apparatus decrypts said content key data and said usage control policy data stored in said distributed module and determines the handling of said content data based on the related decrypted usage control policy data.

2. A data providing system as set forth in claim 1, wherein:

   said data providing apparatus distributes said module storing said content key data and said usage control policy data encrypted using distribution key data to said data processing apparatus and
   said data processing apparatus decrypts said content key data and said usage control policy data stored in said distributed module using said distribution key data.

3. A data providing system as set forth in claim 2, further comprising a management apparatus for managing said distribution key data and distributing said distribution key data to said data providing apparatus and said data processing apparatus.

4. A data providing system as set forth in claim 1, wherein said data providing apparatus generates its own signature data for at least one of said content key data and said usage control policy and distributes said module storing said generated signature data to said data processing apparatus.

5. A data providing system as set forth in claim 4, wherein said data providing apparatus generates said signature data using its own secret key data and distributes said module storing public key data corresponding to said secret key data to said data processing apparatus.

6. A data providing system as set forth in claim 5,

   further comprising a management apparatus for preparing public key certificate data certifying the legitimacy of said public key data, wherein
   said data providing apparatus distributes said module storing said public key certificate data to said data processing apparatus.

7. A data providing system as set forth in claim 1, wherein said data providing apparatus distributes

   a first file storing said content data and
   a second file storing said content key data and said usage control policy
   to said data processing apparatus.

8. A data providing system as set forth in claim 7, wherein said data providing apparatus generates signature data using its own secret key data for the first file and the second file and distributes said module storing said generated signature data to said data processing apparatus.

9. A data providing system as set forth in claim 8, wherein said data processing apparatus distributes said module storing public key data corresponding to said secret key data to said data processing apparatus.

10. A data providing system as set forth in claim 1, wherein said data providing apparatus performs mutual authentication with said data processing apparatus, encrypts said module using session key data obtained by said mutual authentication, and transmits said encrypted module to said data processing apparatus.

11. A data providing system as set forth in claim 1, wherein said data providing apparatus generates a storage medium storing said module.

12. A data providing system as set forth in claim 1, wherein said data processing apparatus determines at least one of a purchase mode and usage mode of said content data based on said usage control policy.

13. A data providing system as set forth in claim 1, wherein said data processing apparatus outputs said decrypted content key data and said encrypted content data to a decryption apparatus.

14. A data providing system as set forth in claim 9, wherein said data processing apparatus verifies the legitimacy of signature data stored in said module using public key data stored in said module.

15. A data providing system as set forth in claim 3, wherein:

said data processing apparatus determines at least one of a purchase mode and usage mode of distributed content data based on usage control policy data and transmits log data indicating a log of at least said determined purchase mode and usage mode and
said management apparatus performs profit distribution processing for distributing profit obtained accompanied with said purchase and said usage of said content data in said data processing apparatus to related parties of said data providing apparatus based on said received log data.

16. A data providing system as set forth in claim 1, wherein said data processing apparatus is comprised of a module making it difficult for the processing content, predetermined data stored in an internal memory, and data being processed from being monitored and tampered with from the outside.

17. A data processing apparatus utilizing content data distributed from a data providing apparatus, which
receives a module storing content data encrypted by using content key data, encrypted content key data, and encrypted usage control policy data indicating the handling of said content data from said data providing apparatus, decrypts said content key data and said usage control policy data stored in the related received module, and determines the handling of said content data based on the related decrypted usage control policy data.

18. A data providing system comprising a data providing apparatus, a data distribution apparatus, and a data processing apparatus, wherein

said data providing apparatus provides a first module storing content data encrypted by using content key data, encrypted content key data, and encrypted usage control policy data indicating the handling of said content data to said data distribution apparatus,
said data distribution apparatus distributes a second module storing said encrypted content data, content key data, and usage control policy data stored in said provided first module to said data processing apparatus, and
said data processing apparatus decrypts said content key data and said usage control policy data stored in said distributed second module and determines the handling of said content data based on the related decrypted usage control policy data.

19. A data providing system as set forth in claim 18, wherein said data distribution apparatus distributes a module storing price data showing a price of said content data to said data processing apparatus.

20. A data providing system as set forth in claim 18, wherein:

said data providing apparatus provides said first module storing said content key data and said usage control policy data encrypted using distribution key data to said data distribution apparatus and
said data processing apparatus decrypts said content key data and said usage control policy data stored in said distributed second module using said distribution key data.

21. A data providing system as set forth in claim 20, further comprising a management apparatus for managing said distribution key data and distributing said distribution key data to said data providing apparatus and said data processing apparatus.

22. A data providing system as set forth in claim 20, wherein

said data providing apparatus generates its own signature data for at least one of said content key data and said usage control policy and provides said first module storing said generated signature data and storing a third module encrypted using said distribution key data to said data distribution apparatus and
said data distribution apparatus stores said provided third module in said second module and distributes it to said data processing apparatus.

23. A data providing system as set forth in claim 22, wherein said data providing apparatus generates said signature data using its own secret key data and provides said third module storing public key data corresponding to said secret key data to said data distribution apparatus.

24. A data providing system as set forth in claim 23,

further comprising a management apparatus for preparing public key certificate data certifying the legitimacy of said public key data, wherein
said data providing apparatus provides said first module storing said third module storing said public key certificate data to said data distribution apparatus.

25. A data providing system as set forth in claim 18, wherein said data providing apparatus provides

a first file storing said content data and
a second file storing said content key data and said usage control policy
to said data distribution apparatus.

26. A data providing system as set forth in claim 25, wherein said data providing apparatus generates signature data using its own secret key data for the first file and the second file and provides said first module storing said generated signature data to said data distribution apparatus.

27. A data providing system as set forth in claim 25, wherein said data processing apparatus provides said first module storing public key data corresponding to said secret key data to said data distribution apparatus.

28. A data providing system as set forth in claim 19, wherein said data distribution apparatus generates signature data using its own secret key data for said price data and stores said signature data in said second module.

29. A data providing system as set forth in claim 28, wherein said data providing apparatus provides said second module storing public key data corresponding to its own secret key data to said data processing apparatus.

30. A data providing system as set forth in claim 26, wherein said data distribution apparatus verifies the signature data of said first file and said second file using public key data of said data providing apparatus.

31. A data providing system as set forth in claim 25, wherein said data providing apparatus provides said first module storing link data showing a linkage of said first file and said second file to said data distribution apparatus.

32. A data providing system as set forth in claim 18, wherein said data distribution apparatus performs mutual authentication with said data processing apparatus, encrypts said second module using session key data obtained by said mutual authentication, and transmits said encrypted second module to said data processing apparatus.

33. A data providing system as set forth in claim 18, wherein said data providing apparatus generates a storage medium storing said module.

34. A data providing system as set forth in claim 18, wherein said data processing apparatus determines at least one of a purchase mode and usage mode of said content data based on said usage control policy.

35. A data providing system as set forth in claim 18, wherein said data processing apparatus outputs said decrypted content key data and said encrypted content data to a decryption apparatus.

36. A data providing system as set forth in claim 29, wherein said data processing apparatus verifies the legitimacy of signature data stored in said second module using public key data stored in said second module.

37. A data providing system as set forth in claim 21, wherein:

said data processing apparatus determines at least one of a purchase mode and usage mode of distributed content data based on usage control policy data and transmits log data indicating a log of at least said determined purchase mode and usage mode and
said management apparatus performs profit distribution processing for distributing profit obtained accompanied with said purchase and said usage of said content data in said data processing apparatus to related parties of said data providing apparatus based on said received log data.

38. A data providing system as set forth in claim 18, wherein said data processing apparatus is comprised of a module making it difficult for the processing content, predetermined data stored in an internal memory, and data being processed from being monitored and tampered with from the outside.

39. A data providing system comprising a data providing apparatus, at least a first data distribution apparatus and a second data distribution apparatus, and a data processing apparatus, wherein

said data providing apparatus provides a first module storing content data encrypted by using content key data, encrypted content key data, and encrypted usage control policy data indi-

cating the handling of said content data to said plurality of data distribution apparatuses,
said first data distribution apparatus distributes the second module storing said encrypted content data, content key data, and usage control policy data stored in said provided first module to said data processing apparatus,
said second data distribution apparatus distributes a third module storing said encrypted content data, content key data, and usage control policy data stored in said provided first module to said data processing apparatus, and
said data processing apparatus decrypts said content key data and said usage control policy data stored in said distributed second module and said third module and determines the handling of said content data based on the related decrypted usage control policy data.

40. A data providing system comprising at least a first data providing apparatus and a second data providing apparatus, a data distribution apparatus, and a data processing apparatus, wherein

said first data providing apparatus provides a first module storing first content data encrypted by using first content key data, encrypted first content key data, and encrypted first usage control policy data indicating the handling of said first content data to said data distribution apparatus,
said second data providing apparatus provides a second module storing second content data encrypted by using second content key data, encrypted second content key data, and encrypted second usage control policy data indicating the handling of said second content data to said data distribution apparatus,
said data distribution apparatus distributes a third module storing said encrypted first content data, said first content key data, and said first usage control policy data stored in said provided first module and said encrypted second content data, said second content key data, and said second usage control policy data stored in said provided second module to said data processing apparatus, and
said data processing apparatus decrypts said first content key data and said first usage control policy data stored in said distributed third module, determines the handling of said first content data based on the related decrypted first usage control policy data, decrypts said second content key data and said second usage control policy data stored in said distributed third module, and determines the handling of said second content data based on the related decrypted second usage control policy data.

41. A data providing apparatus for distributing content data to a data processing apparatus for using the content data, which

distributes a module storing content data encrypted by using the content key data, encrypted content key data, and encrypted usage control policy data indicating the handling of said content data to said data processing apparatus.

42. A data providing apparatus as set forth in claim 41 preparing said usage control policy and distributing said module storing said generated usage control policy to said data processing apparatus.

43. A data providing apparatus as set forth in claim 41, which distributes said module storing said content key data and said usage control policy data encrypted using distribution key data to said data processing apparatus.

44. A data providing apparatus as set forth in claim 43, which encrypts said content key data Kc and said usage control policy data using said distribution key data issued by a predetermined authority manager.

45. A data providing apparatus as set forth in claim 41, which generates its own signature data for at least one of said content data, content key data, and usage control policy data and distributes said module storing said generated signature data to said data processing apparatus.

46. A data providing apparatus as set forth in claim 45, which generates said signature data using its own secret key data and distributes said module storing public key data corresponding to said secret key data to said data processing apparatus.

47. A data providing apparatus as set forth in claim 46, which distributes said module storing public key certificate data certifying the legitimacy of said public key data to said data processing apparatus.

48. A data providing apparatus as set forth in claim 41, which distributes:

a first file storing said content data and
a second file storing said content key data and said usage control policy data
to said data processing apparatus.

49. A data providing apparatus as set forth in claim 48, which generates signature data using its own secret key data for said first file and said second file and distributes said module storing said generated signature data to said data processing apparatus.

50. A data providing apparatus as set forth in claim 49,

which distributes said module storing public key data corresponding to said secret key data to said data processing apparatus.

51. A data providing apparatus as set forth in claim 41, which performs mutual authentication with said data processing apparatus, encrypts said module using session key data obtained by said mutual authentication, and transmits said encrypted module to said data processing apparatus.

52. A data providing apparatus as set forth in claim 41, which generates a storage medium storing said module.

53. A data providing apparatus as set forth in claim 41, which defines said module by an application layer.

54. A data providing apparatus as set forth in claim 53, which uses a presentation layer and transport layer under said application layer as distribution protocol for distributing said module to said data processing apparatus.

55. A data providing apparatus as set forth in claim 41, which defines said module by a format not dependent on a medium for distributing said module to said data processing apparatus.

56. A data providing method for distributing data from a data providing apparatus to a data processing apparatus, comprising the steps of:

distributing a module storing content data encrypted by using content key data, encrypted content key data, and encrypted usage control policy data indicating the handling of said content data from said data providing apparatus to said data processing apparatus and
decrypting said content key data and said usage control policy data stored in said distributed module and determining the handling of said content data based on the related decrypted usage control policy data at said data processing apparatus.

57. A data providing method as set forth in claim 56, further comprising the steps of:

distributing said module storing said content key data and said usage control policy data encrypted using distribution key data from said data providing apparatus to said data processing apparatus and
decrypting said content key data and said usage control policy stored in said distributed module using said distribution key data.

58. A data providing method using a data providing apparatus, data distribution apparatus, and data processing apparatus, comprising the steps of:

providing a first module storing content data encrypted by using content key data, encrypted content key data, and encrypted usage control policy data indicating the handling of said content data from said data providing apparatus to said data distribution apparatus,
distributing a second module storing said encrypted content data, content key data, and usage control policy data stored in said provided first module from said data distribution apparatus to said data processing apparatus, and
decrypting said content key data and said usage control policy data stored in said distributed second module and determining the handling of said content data based on the related decrypted usage control policy data at said data processing apparatus.

59. A data providing method as set forth in claim 58, which distributes said second module storing price data showing a price of said content data from said data distribution apparatus to said data processing apparatus.

60. A data providing method using a data providing apparatus, at least a first data distribution apparatus and second data distribution apparatus, and a data processing apparatus, comprising the steps of:

providing a first module storing content data encrypted by using content key data, encrypted content key data, and encrypted usage control policy data indicating the handling of said content data from said data providing apparatus to said data distribution apparatuses,
distributing a second module storing said encrypted content data, content key data, and usage control policy data stored in said provided first module from said first data distribution apparatus to said data processing apparatus,
distributing a third module storing said encrypted content data, content key data, and usage control policy data stored in said provided first module from said second data distribution apparatus to said data processing apparatus, and
decrypting said content key data and said usage control policy data stored in said distributed second module and said third module and determining the handling of said content data based on the related decrypted usage control policy data at said data processing apparatus.

61. A data providing method using at least a first data providing apparatus and second data providing ap-

paratus, a data distribution apparatus, and a data processing apparatus, comprising the steps of:

providing a first module storing first content data encrypted by using first content key data, encrypted first content key data, and encrypted first usage control policy data indicating the handling of said first content data from said first data providing apparatus to said data distribution apparatus,
providing a second module storing second content data encrypted by using second content key data, encrypted second content key data, and encrypted second usage control policy data indicating the handling of said second content data from said second data providing apparatus to said data distribution apparatus,
distributing a third module storing said encrypted first content data, said first content key data, and said first usage control policy data stored in said provided first module and said encrypted second content data, said second content key data, and said second usage control policy data stored in said provided second module from said data distribution apparatus to said data processing apparatus, and
decrypting said first content key data and said first usage control policy data stored in said distributed third module, determining the handling of said first content data based on the related decrypted first usage control policy data, decrypting said second content key data and said second usage control policy data stored in said distributed third module, and determining the handling of said second content data based on the related decrypted second usage control policy data at said data processing apparatus

62. A data providing method for distributing content data to a data processing apparatus using said content data, which

distributes a module storing content data encrypted using content key data, said encrypted content key data, and encrypted usage control policy data showing the handling of said content data.

63. A data providing method as set forth in claim 62, which distributes said module storing said content key data and said usage control policy data encrypted using distribution key data to said data processing apparatus.

64. A data providing method as set forth in claim 62, which generates its own signature data for at least one of said content data, said content key data, and said usage control policy data and distributes said module storing said generated signature data to said data processing apparatus.

65. A data providing method as set forth in claim 64, which generates said signature data using its own secret key data and distributes said module storing public key data corresponding to said secret key data to said data processing apparatus.

66. A data providing method as set forth in claim 65, which distributes said module storing public key certificate data certifying the legitimacy of said public key data to said data processing apparatus.

67. A data providing method as set forth in claim 62, which distributes:

a first file storing said content data and
a second file storing said content key data and said usage control policy data
to said data processing apparatus.

68. A data providing method as set forth in claim 67, which generates signature data using its own secret key data for said first file and said second file and stores said generated signature data.

69. A data providing method as set forth in claim 68, which distributes a module storing public key data corresponding to said secret key data to said data processing apparatus.

70. A data providing method as set forth in claim 62, which performs mutual authentication with said data processing apparatus, encrypts said module using session key data obtained by said mutual authentication, and transmits said encrypted module to said data processing apparatus.

71. A data providing method as set forth in claim 62, which generates a storage medium storing said module.

72. A data providing system comprising a data providing apparatus, data processing apparatus, and management apparatus, wherein

said data providing apparatus distributes content data and usage control policy data indicating the handling of the related content data to said data processing apparatus and requests to said management apparatus to certify legitimacy of said usage control policy data,
said data processing apparatus uses said distributed content data based on said distributed usage control policy data, and
said management apparatus manages said data providing apparatus and said data processing apparatus and certifies the legitimacy of said usage control policy data in response to a request from said data providing apparatus.

73. A data providing system as set forth in claim 72, wherein said data providing apparatus makes said request by transmitting to said management apparatus a module storing said usage control policy data, its own identifier, and signature data generated using its own secret key data for at least said usage control policy data.

74. A data providing system as set forth in claim 73, wherein

said management apparatus distributes public key certificate data for certifying the legitimacy of the public key data corresponding to said secret key data of said data providing apparatus to said data providing apparatus together with the signature data generated by using its own secret key data, and
said data providing apparatus makes a request by transmitting a module storing said public key certificate data, said usage control policy data, its own identifier, and said signature data to said management apparatus.

75. A data providing system as set forth in claim 72, wherein:

said management apparatus manages distribution key data, distributes the related distribution key data to said data processing apparatus, generates signature data generated by using its own secret key data with respect to said usage control policy data in response to a request from said data providing apparatus, encrypts a module storing the related generated signature data and said usage control policy data by using said distribution key data, and transmits the same to said data providing apparatus,
said data providing apparatus distributes a module received from said management apparatus to said data processing apparatus, and
said data processing apparatus decrypts said module received from said data providing apparatus by using said distribution key data, verifies the legitimacy of said signature data stored in the related module by using the public key data of said management apparatus, and uses said distributed content data based on the usage control policy data stored in said module when it decides it is legitimate.

76. A data providing system as set forth in claim 72, wherein:

said data processing apparatus determines at least one of a purchase mode and usage mode of distributed content data based on usage control policy data and transmits log data indicating a log of at least said determined purchase mode and usage mode and
said management apparatus performs profit distribution processing for distributing profit obtained accompanied with said purchase and said usage of said content data in said data processing apparatus to related parties of said data providing apparatus based on said received log data.

77. A data providing system comprising a data providing apparatus, data processing apparatus, and management apparatus, wherein

said data providing apparatus encrypts content data by using content key data, distributes the related encrypted content data to said data processing apparatus, and requests to said management apparatus to certify the legitimacy of said content key data,
said data processing apparatus decrypts said distributed content data by using said content key data and uses the related decrypted content data, and
said management apparatus manages said data providing apparatus and said data processing apparatus and certifies the legitimacy of said content key data in response to a request from said data providing apparatus.

78. A data providing system as set forth in claim 77, wherein said data providing apparatus distributes a module storing said content data and said content key data to said data processing apparatus.

79. A management apparatus for managing a data providing apparatus for distributing content data and usage control policy data indicating the handling of the related content data and a data processing apparatus for using said distributed content data based on said distributed usage control policy data, which

certifies the legitimacy of said usage control policy data in response to a request from said data providing apparatus.

80. A data providing system as set forth in claim 79, which manages public key data corresponding to secret key data of said data providing apparatus when receiving from said data providing apparatus said request using a module storing said usage control policy data, an identifier of said data providing apparatus, and signature data generated using secret key data of said data providing apparatus for at least said usage control policy data.

81. A data providing system as set forth in claim 80,

which transmits public key certificate data certifying the legitimacy of said public key data to said data providing apparatus.

82. A management apparatus for managing a data providing apparatus for distributing content data and usage control policy data indicating the handling of the related content data encrypted using content key data and a data processing apparatus for using said distributed content data afer decrypting said distributed content data using said content key data based on said distributed usage control policy data, which

certifies the legitimacy of said content key data in response to a request from said data providing apparatus.

83. A data providing system comprising a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus, wherein

said data providing apparatus provides content data and usage control policy data indicating the handling of the related content data to said data distribution apparatus and requests to said management apparatus to certify the legitimacy of said usage control policy data,
said data distribution apparatus distributes said provided content data and said usage control policy data to said data processing apparatus,
said data processing apparatus uses said distributed content data based on said distributed usage control policy data, and
said management apparatus manages said data providing apparatus and said data processing apparatus and certifies the legitimacy of said usage control policy data in response to a request from said data providing apparatus.

84. A data providing system as set forth in claim 83, wherein said data providing apparatus makes said request by transmitting to said management apparatus a module storing an identifier of said content data, said usage control policy data, and signature data generated using its own secret key data for at least said usage control policy data.

85. A data providing system as set forth in claim 84, wherein said management apparatus distributes public key certificate data certifying the legitimacy of public key data corresponding to said secret key data of said data providing apparatus together with signature data generated using its own secret key data to said data providing apparatus.

86. A data providing system as set forth in claim 84, wherein said

said management apparatus manages distribution key data, distributes the related distribution key data to said data processing apparatus, generates signature data generated by using its own secret key data with respect to said usage control policy data in response to a request from said data providing apparatus, encrypts a module storing the related generated signature data and said usage control policy data by using said distribution key data, and transmits the same to said data providing apparatus,
said data providing apparatus distributes a module received from said management apparatus to said data distribution apparatus, and
said data processing apparatus decrypts said module distributed said data distribution apparatus, verifies the legitimacy of said signature data stored in the related module by using the public key data of said management apparatus, and uses said distributed content data based on the usage control policy data stored in said module when it decides it is legitimate.

87. A data providing system as set forth in claim 83, wherein:

said data distribution apparatus distributes price data indicating the price of said distributed content data to said data processing apparatus and
said management apparatus certifies the legitimacy of said price data in response to a request from said data distribution apparatus.

88. A data providing system as set forth in claim 83, wherein

said data processing apparatus determines at least one of a purchase mode and usage mode of distributed content data based on said usage control policy data and transmits log data indicating a log of at least said determined purchase mode and usage mode to said management apparatus and
said management apparatus performs profit distribution processing for distributing profit obtained accompanied with said purchase and said usage of said content data in said data processing apparatus to related parties of said data providing apparatus and said data distribution apparatus based on said received log data.

89. A data providing system as set forth in claim 83, wherein

said data processing apparatus has a first mod-

ule communicating with said data distribution apparatus and a second module determining at least one of a purchase mode and usage mode of distributed content data based on said distributed usage control policy data and transmitting log data indicating a log of at least said determined purchase mode and usage mode to said management apparatus and
said management apparatus manages the data providing apparatus, data distribution apparatus, and data processing apparatus and performs profit distribution processing for distributing profit obtained accompanied with said data processing apparatus receiving distribution of said content data and purchasing and using said content data to related parties of said data providing apparatus and said data distribution apparatus based on said received log data received from said second module.

90. A data providing system comprising a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus, wherein

said data providing apparatus encrypts content data by using content key data, provides related encrypted content data, and usage control policy data indicating the handling of the related content data to said data distribution apparatus, and requests to said management apparatus to certify the legitimacy of said content key data,
said data distribution apparatus distributes said provided content data and said usage control policy data to said data processing apparatus,
said data processing apparatus uses said content data containing the decryption of said content data using said content key data based on said distributed usage control policy data, and
said management apparatus manages said data providing apparatus and said data processing apparatus and certifies the legitimacy of said content key data in response to a request from said data providing apparatus.

91. A data providing system as set forth in claim 90, wherein said data providing apparatus encrypts said content key data and provides a module storing said encrypted content key data and encrypted content data to said data distribution apparatus.

92. A management apparatus for managing a data providing apparatus for providing content data and usage control policy data indicating the handling of the related content data, a data distribution apparatus for distributing said provided content data and said usage control policy data, and a data processing apparatus for using said distributed content data based on said distributed usage control policy data, which

certifies the legitimacy of said usage control policy data in response to a request from said data providing apparatus.

93. A management apparatus as set forth in claim 92, which certifies the legitimacy of said content key data in response to a request from said data providing apparatus when encrypting said content data using content key data and providing it from said data providing apparatus to said data distribution apparatus.

94. A management apparatus as set forth in claim 92, which certifies the legitimacy of said price data in response to a request from said data distribution apparatus when distributing said price data from said data distribution apparatus to said data processing apparatus together with said content data and said usage control policy data.

95. A data providing method using a data providing apparatus, data processing apparatus, and management apparatus, comprising the steps of:

distributing content data and usage control policy data indicating the handling of the related content data from said data providing apparatus to said data processing apparatus and
using said distributed content data based on said distributed usage control policy data at said data processing apparatus, and
certifying the legitimacy of said usage control policy data in said management apparatus in response to a request from said data providing apparatus.

96. A data providing method using a data providing apparatus, data processing apparatus, and management apparatus, comprising the steps of:

distributing content data encrypted by using content key data from said data providing apparatus to said data processing apparatus,
decrypting said distributed content data by using said content key data at said data processing apparatus, and
certifying the legitimacy of said content key data in said management apparatus in response to a request from said data providing apparatus.

97. A data providing method using a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus, comprising the steps of:

providing content data and usage control policy data indicating the handling of the related content data from said data providing apparatus to said data distribution apparatus,
distributing said provided content data and said usage control policy data from said data distribution apparatus to said data processing apparatus,
using said distributed content data based on said distributed usage control policy data at said data processing apparatus, and
certifying the legitimacy of said usage control policy data in said management apparatus in response to a request from said data providing apparatus.

98. A data providing method using a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus, comprising the steps of:

providing content data encrypted by using content key data and usage control policy data indicating the handling of the related content data from said data providing apparatus to said data distribution apparatus,
distributing said content data and said usage control policy data provided from said data distribution apparatus to said data processing apparatus to said data processing apparatus,
using said content data containing the decryption of said content data using said content key data based on said distributed usage control policy data in said data processing apparatus, and
certifying the legitimacy of said content key data in said management apparatus in response to a request from said data providing apparatus.

99. A data providing system comprising a data providing apparatus, data processing apparatus, and management apparatus, wherein

said data providing apparatus distributes content data and usage control policy data indicating the handling of the related content data to said data processing apparatus,
said data processing apparatus determines at least one of a purchase mode and a usage mode of said distributed content data based on said distributed usage control policy data and transmits log data indicating the log of at least one of the related determined purchase mode and usage mode to said management apparatus, and
said management apparatus manages said data providing apparatus and said data processing apparatus and performs profit distribution processing for distributing the profit obtained accompanied with said purchase and said usage of said content data in said data processing apparatus to related parties of said data providing apparatus based on received log data.

100. A data providing system as set forth in claim 99, wherein

said data providing apparatus encrypts said content data using predetermined key data and distributes it to said data processing apparatus,
said data processing apparatus decrypts said received content data using said key data, and
said management apparatus manages said key data.

101. A data providing system as set forth in claim 99, wherein

said data providing apparatus generates predetermined key data and registers said generated key data to said management apparatus,
said management apparatus manages said registered key data and transmits corresponding key data to said data processing apparatus when processing for purchasing of content data is performed in said data processing apparatus, and
said data processing apparatus decrypts said received content data using said received key data.

102. A data providing system as set forth in claim 100, wherein said data providing apparatus encrypts said key data and distributes a module storing said encrypted key data, encrypted content data, and said usage control policy data to said data processing apparatus.

103. A data providing system as set forth in claim 102, wherein

said management apparatus manages distribution key data and distributes said distribution key data to said data providing apparatus and said data processing apparatus,
said data providing apparatus encrypts said key data and said usage control policy data using said distributed distribution key data, and
said data processing apparatus decrypts said key data and said usage control policy data using said distributed distribution key data.

104. A data providing system as set forth in claim 103, wherein said management apparatus distributes a plurality of distribution key data having predeter-

mined terms of validity to said data providing apparatus and said data processing apparatus for exactly a predetermined period.

105. A data providing system as set forth in claim 102, wherein

said data providing apparatus generates signature data for at least one of said encrypted content data and usage control policy data using its own secret key data and distributes a module storing said encrypted content data, said encrypted key data, said encrypted usage control policy data, and said signature data to said data processing apparatus,
said data processing apparatus verifies said signature data stored in said distributed module using public key data corresponding to said secret key data, and
said management apparatus manages said public key data.

106. A data providing system as set forth in claim 105, wherein said data providing apparatus distributes said module storing public key data corresponding to its own secret key data to said data processing apparatus.

107. A data providing system as set forth in claim 105, wherein said management apparatus distributes said module storing public key data corresponding to said secret key data of said data providing apparatus to said data processing apparatus.

108. A data providing system as set forth in claim 99, wherein

said management apparatus distributes distribution key data to said data providing apparatus and said data processing apparatus,
said data providing apparatus encrypts said usage control policy using said distribution key data and distributes it to said data processing apparatus, and
said data processing apparatus decrypts said received usage control policy data using said distribution key data.

109. A data providing system as set forth in claim 100, wherein said management apparatus authenticates the legitimacy of at least one of said usage control policy data and said key data.

110. A data providing system as set forth in claim 99, wherein said management apparatus generates settlement claim data used when claiming settlement processing in accordance with said profit distribution processing, adds signature data based on its own secret key data to said settlement claim data, and transmits it to an apparatus performing said settlement processing or said data providing apparatus.

111. A data providing system as set forth in claim 99, wherein said management apparatus performs processing for registration of said data processing apparatus, manages said registered data processing apparatus, and performs profit distribution processing based on said log data received from said registered data processing apparatus.

112. A data providing system as set forth in claim 99, wherein said data processing apparatus determines a purchase mode of said distributed content data based on said usage control policy data, generates usage control status data in accordance with said determined purchase mode, and controls usage of said distributed content data based on said usage control status data.

113. A data providing system as set forth in claim 99, wherein said data processing apparatus is comprised of a module making it difficult for the processing content, predetermined data stored in an internal memory, and data being processed from being monitored and tampered with from the outside.

114. A management apparatus for managing a data providing apparatus for distributing content data and usage control policy data indicating the handling of said content data and a data processing apparatus for determining at least one of a purchase mode and usage mode of said distributed content data based on said distributed usage control policy data and generating log data showing a log of at least one of said determined purchase mode and usage mode, which

receives said log data from said data processing apparatus and performs profit distribution processing for distributing the profit accompanied with said purchase and said usage of said content data in said data processing apparatus to related parties of said data providing apparatus based on said received log data.

115. A management apparatus as set forth in claim 113, which manages key data when distributing content data encrypted using predetermined key data from said data providing apparatus to said data processing apparatus.

116. A management apparatus as set forth in claim 114, which authenticates the legitimacy of at least one of said usage control policy data and key data used when decrypting said content data.

117. A data providing apparatus for receiving distribution of content data and usage control policy data indicating the handling of the related content data from a data providing apparatus and transmitting log data to a management apparatus for performing profit distribution processing for distributing the profit obtained accompanied with the purchase and usage of the related distributed content data to related parties of said data providing apparatus based on predetermined log data, which

determines at least one of a purchase mode and usage mode of said distributed content data based on said distributed usage control policy data and transmits said log data indicating the log of the determined designation mode and usage mode to said management apparatus.

118. A data providing apparatus as set forth in claim 117, which receives said key data from said data providing apparatus when said content data is encrypted using predetermined key data.

119. A data processing apparatus as set forth in claim 117, comprised of a module making it difficult for the processing content, predetermined data stored in an internal memory, and data being processed from being monitored and tampered with from the outside.

120. A data providing system comprising a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus, wherein

said data providing apparatus provides content data and usage control policy data indicating the handling of the related content data to said data distribution apparatus,
said data distribution apparatus distributes said provided content data and said usage control policy data to said data processing apparatus,
said data processing apparatus has a first module for communicating with said data distribution apparatus and a second module for determining at least one of a purchase mode and usage mode of said distributed content data based on said distributed usage control policy data and transmitting log data indicating the log of the related determined purchase mode and usage mode to said management apparatus, and
said management apparatus manages the data providing apparatus, data distribution apparatus, and data processing apparatus and performs profit distribution processing for distributing the profit obtained accompanied with said data processing apparatus receiving said distribution of said content data and purchasing and using said content data to related parties of said data providing apparatus and said data distribution apparatus based on said log data received from said second module.

121. A data providing system as set forth in claim 120, wherein said data providing apparatus encrypts said content data using content key data and provides it to said data distribution apparatus.

122. A data providing system as set forth in claim 120, wherein said data distribution apparatus generates price data showing the price of said distributed content data and distributes said price data to said data processing apparatus.

123. A data providing system as set forth in claim 120, wherein

said data providing apparatus encrypts said content key data and said usage control policy by using distribution key data and provides it to said data distribution apparatus,
said data processing apparatus decrypts said content key data and said usage control policy using said distribution key data, and
said management apparatus manages said distribution key data and distributes said distribution key data to said data providing apparatus and said data processing apparatus.

124. A data providing system as set forth in claim 123, wherein

said data providing apparatus generates first signature data for at least one of said encrypted content data, said encrypted content key data, and said encrypted usage control policy data using its own first secret key data and provides a first module storing said encrypted content data, said encrypted key data, said encrypted usage control policy data, and said first signature data to said data distribution apparatus,
said data distribution apparatus verifies said first signature data using first public key data corresponding to said first secret key data, then stores second signature data generated using its own second secret key data in said first module to generate a second module and distributes said second module to said data processing apparatus,
said data processing apparatus verifies said first signature data stored in said distributed second module using said first public key data and verifies said second signature data stored in said distributed second module using second public key data corresponding to said second secret key data, and

said management apparatus manages said first public key data and said second public key data.

125. A data providing system as set forth in claim 124, wherein

said data providing apparatus provides said first module storing said first public key data to said data distribution apparatus and
said data distribution apparatus distributes said second module storing said first public key data and said second public key data to said data processing apparatus.

126. A data providing system as set forth in claim 124, wherein said management apparatus distributes said first public key data and said second public key data to said data processing apparatus.

127. A data providing system as set forth in claim 120, wherein

said data distribution apparatus distributes price data showing the price of said distributed content data to said data processing apparatus and
said management apparatus authenticates the legitimacy of the data of at least one of key data used when encrypting said content data and said price data.

128. A data providing system as set forth in claim 120, wherein said data distribution apparatus distributes to said data processing apparatus a module storing said provided encrypted content data, said provided usage control policy data, said key data encrypting said content data, and price data showing the price of said distributed content data.

129. A data providing system as set forth in claim 120, wherein said management apparatus performs profit distribution processing for distributing profit obtained accompanied with said data processing apparatus receiving distribution of said content data and purchasing and using said content data to related parties of said data providing apparatus and said data distribution apparatus, generates settlement claim data to be used when claiming settlement, add its own signature data to said settlement claim data, and transmits this to an apparatus for performing said settlement processing.

130. A data providing system as set forth in claim 129, wherein said management apparatus transmits settlement report data showing the results of said profit distribution processing to at least one of said data providing apparatus and said data distribution apparatus.

131. A data providing system as set forth in claim 120, wherein said management apparatus performs profit distribution processing for distributing profit obtained accompanied with said data processing apparatus receiving distribution of said content data and purchasing and using said content data to related parties of said data providing apparatus and said data distribution apparatus, generates settlement claim data to be used when claiming settlement, adds its own signature data to said settlement claim data, and transmits this to at least one of said data providing apparatus and said service providing apparatus.

132. A data providing system as set forth in claim 120, wherein said management apparatus performs processing for registration of said data processing apparatus, manages said registered data processing apparatus, and performs said profit distribution processing based on said log data received from said registered data processing apparatus.

133. A data providing system as set forth in claim 120, wherein said data processing apparatus determines at least one of a purchase mode and usage mode of said distributed content data based on said usage control policy data, generates usage control status data in accordance with said determined purchase mode and usage mode, and controls usage of said distributed content data based on said usage control status data.

134. A data providing system as set forth in claim 120, wherein said second module of said data processing apparatus is a module making it difficult for the processing content, predetermined data stored in an internal memory, and data being processed from being monitored and tampered with from the outside.

135. A management apparatus for managing a data providing apparatus for providing content data and usage control policy data indicating the handling of the related content data, a data distribution apparatus for distributing said provided content data and said usage control policy data, and a data processing apparatus for determining at least one of a purchase mode and usage mode of said distributed content data based on said distributed usage control policy data and creating log data indicating the log of at least one of the related determined purchase mode and usage mode, which

performs profit distribution processing for distributing the profit obtained accompanied with said data processing apparatus receiving said distribution of said content data and purchasing and using

said content data to related parties of said data providing apparatus and said data distribution apparatus based on said received log data.

136. A management apparatus as set forth in claim 135, which manages said key data when distributing said content data encrypted using predetermined content key data from said data providing apparatus to said data processing apparatus.

137. A management apparatus as set forth in claim 136, which authenticates the legitimacy of at least one of said usage control policy data and said content key data.

138. A data processing apparatus for receiving distribution of content data and usage control policy data from a data distribution apparatus receiving the provision of content data and usage control policy data indicating the handling of the related content data from a data providing apparatus and transmitting log data to a management apparatus for performing profit distribution processing for distributing the profit obtained accompanied with the purchase and usage of said distributed content data to related parties of said data providing apparatus and said data distribution apparatus based on predetermined log data, which has

a first module for communicating with said data distribution apparatus and
a second module for determining at least one of a purchase mode and usage mode of said distributed content data based on said distributed usage control policy data and transmitting log data indicating the log of the related determined purchase mode and usage mode to said management apparatus.

139. A data processing apparatus as set forth in claim 138, which is a module making it difficult for the processing content, predetermined data stored in an internal memory, and data being processed from being monitored and tampered with from the outside.

140. A data providing system comprising a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus, wherein

said data providing apparatus provides content data and usage control policy data indicating the handling of the related content data to said data distribution apparatus,
said data distribution apparatus distributes said provided content data and said usage control policy data to said data processing apparatus and performs charge processing concerning the distribution of said content data based on a data distribution apparatus use purchase log data received from said data processing apparatus,
said data processing apparatus has a first module for creating the data distribution apparatus use purchase log data indicating the log of the purchase of said content data distributed from said data distribution apparatus and transmitting the same to said data distribution apparatus and a second module for determining at least one of the purchase mode and the usage mode of said distributed content data based on said distributed usage control policy data and transmitting a management apparatus use log data indicating the log of the related determined purchase mode and usage mode to said management apparatus, and
said management apparatus performs profit distribution processing for distributing the profit obtained accompanied with said purchase and said usage of said content data in said data processing apparatus to related parties of said data providing apparatus and said data distribution apparatus based on said management apparatus use log data.

141. A data processing apparatus for receiving the distribution of content data and usage control policy data indicating the handling of the related content data from a data providing apparatus via a data distribution apparatus and transmitting said log data to a management apparatus for performing profit distribution processing for distributing the profit obtained accompanied with the purchase and usage of the related distributed content data to related parties of said data providing apparatus and said data distribution apparatus based on said management apparatus use log data, said data processing apparatus comprising,

a first module for creating data distribution apparatus use purchase log data indicating the log of the purchase of said content data distributed from said data distribution apparatus and transmitting the same to said data distribution apparatus and
a second module for determining at least one of a purchase mode and usage mode of said distributed content data based on said distributed usage control policy data and transmitting said management apparatus use log data indicating the log of the related determined purchase mode and usage mode to said management apparatus.

142. A data providing system comprising a data provid-

ing apparatus, data distribution apparatus, data processing apparatus, and a management apparatus, wherein:

said data providing apparatus provides the content data to said data distribution apparatus,
said data distribution apparatus distributes said provided content data to said data processing apparatus,
said data processing apparatus uses said distributed content data, and
said management apparatus manages operation of a data providing service by said data providing apparatus, said data distribution apparatus, and said data processing apparatus.

143. A data providing system as set forth in claim 142, wherein:

said data providing apparatus provides usage control policy data indicating the handling of said content data to said data distribution apparatus,
said data distribution apparatus distributes said provided content data and usage control policy data to said data processing apparatus,
said data processing apparatus uses said distributed content data based on said distributed usage control policy data, and
said management apparatus plays the role of a sub-certificate authority present hierarchically under a route certificate authority, generates and manages public key certificate data to be used when certifying the legitimacy of public key data corresponding to secret key data to be used at said registered data providing apparatus, data distribution apparatus, and data processing apparatus, authenticates said usage control policy data, and performs right processing relating to said content data.

144. A data providing system as set forth in claim 143, wherein

said data providing apparatus encrypts using said key data and provides the result to said data distribution apparatus and
said management apparatus manages said key data.

145. A data providing system as set forth in claim 143, wherein

each of said data providing apparatus and said data distribution apparatus generates its own secret key data to be used for authentication with another apparatus, manages said generated secret key data, generates public key data corresponding to said secret key data, and registers said public key data, identification card, and settlement account to said management apparatus and
said management apparatus generates public key certificate data certifying the legitimacy of said public key data.

146. A data providing system as set forth in claim 145, wherein said management apparatus allocates identification numbers to said data providing apparatus and said data distribution apparatus in accordance with said registration and transmits to said data providing apparatus and said data distribution apparatus public key data of a route certificate authority and public key data of the management apparatus.

147. A data providing system as set forth in claim 145, wherein each of said data providing apparatus and said data distribution apparatus further registers said secret key data in said management apparatus.

148. A data providing system as set forth in claim 143, wherein said data processing apparatus has stored in it in advance secret key data generated by said management apparatus and public key data corresponding to said secret key data.

149. A data providing system as set forth in claim 148, wherein said data processing apparatus has stored in it in advance public key certificate data certifying the legitimacy of said public key data generated by said management apparatus.

150. A data providing system comprising a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus, wherein

said data providing apparatus provides content data to said data distribution apparatus,
said data distribution apparatus distributes said provided content data to said data processing apparatus,
said data processing apparatus uses said distributed content data, and
said management apparatus manages the operation of a data providing service by said data providing apparatus, said data distribution apparatus, and said data processing apparatus, wherein
the transmission of data among said data providing apparatus, said data distribution apparatus, said data processing apparatus, and said management apparatus is carried out by using mutual authentication using a public key en-

cryption method, signature creation, signature verification, and encryption of data by a common key encryption method.

151. A data providing system comprising a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus, wherein

said data providing apparatus provides content data to said data distribution apparatus,
said data distribution apparatus distributes said provided content data to said data processing apparatus,
said data processing apparatus uses said distributed content data, and
said management apparatus manages the operation of a data providing service by said data providing apparatus, said data distribution apparatus, and said data processing apparatus, generates signature data indicating that the related data is generated by itself by using its own secret key data when each of said data providing apparatus, said data distribution apparatus, and said data processing apparatus supplies the data to another apparatus, and generates and manages public key certificate data of public key data corresponding to secret key data of said data providing apparatus, said data distribution apparatus, and said data processing apparatus when the legitimacy of the signature data corresponding to the data is verified by using the public key data of the related other apparatus when receiving the supply of the related data from the other apparatus, wherein
said data providing apparatus, said data distribution apparatus, and said data processing apparatus acquire said their own public key certificate data from said management apparatus before communicating with the other apparatus and transmit the related acquired public key certificate data to said other apparatus.

152. A data providing system comprising a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus, wherein

said data providing apparatus provides content data to said data distribution apparatus,
said data distribution apparatus distributes said provided content data to said data processing apparatus,
said data processing apparatus uses said distributed content data, and
said management apparatus manages the operation of a data providing service by said data providing apparatus, said data distribution apparatus, and said data processing apparatus, generates the signature data indicating that the related data is generated by itself by using its own secret key data when each of said data providing apparatus, said data distribution apparatus, and said data processing apparatus supplies data to another apparatus, and generates and manages public key certificate data of public key data corresponding to secret key data of said data providing apparatus, said data distribution apparatus, and said data processing apparatus when the legitimacy of the signature data corresponding to the data is verified by using the public key data of the related other apparatus when receiving the supply of the related data from the other apparatus, wherein
said data providing apparatus, said data distribution apparatus, and said data processing apparatus acquire their own public key certificate data from said management apparatus before communicating with the other apparatus and transmit the related acquired public key certificate data to said other apparatus at said communication.

153. A data providing system comprising a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus, wherein:

said data providing apparatus provides content data to said data distribution apparatus,
said data distribution apparatus distributes said provided content data to said data processing apparatus,
said data processing apparatus uses said distributed content data, and
said management apparatus manages the operation of a data providing service by said data providing apparatus, said data distribution apparatus, and said data processing apparatus, generates signature data indicating that the related data is generated by itself by using its own secret key data when each of said data providing apparatus, said data distribution apparatus, and said data processing apparatus supplies data to another apparatus, generates and manages public key certificate data of public key data corresponding to secret key data of said data providing apparatus, said data distribution apparatus, and said data processing apparatus when the legitimacy of the signature data corresponding to the data is verified by using the public key data of the related other apparatus when receiving the supply of the related data from the other apparatus, and generates public key certificate revocation list for specifying public key certificate data to be invalidated among

said generated public key certificate data and thereby to restrict said communication or said distribution using public key certificate data specified by said public key certificate revocation list by said data providing apparatus, said data distribution apparatus, and said data processing apparatus.

154. A data providing system as set forth in claim 153, wherein said management apparatus generates public key certificate revocation list specifying public key certificate data corresponding to said data providing apparatus, said data distribution apparatus, and said data processing apparatus used for illegal actions.

155. A data providing system comprising a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus, wherein:

said data providing apparatus provides content data to said data distribution apparatus,
said data distribution apparatus distributes said provided content data to said data processing apparatus,
said management apparatus manages the operation of a data providing service by said data providing apparatus, said data distribution apparatus, and said data processing apparatus, generates signature data indicating that the related data is generated by an apparatus itself by using its own secret key data when said data providing apparatus supplies data to another apparatus, generates and manages public key certificate data of public key data corresponding to secret key data of said data providing apparatus for when another apparatus verifies the legitimacy of the related signature data by using the public key data corresponding to said secret key data, generates public key certificate revocation list for specifying public key certificate data to be invalidated among said generated public key certificate data, distributes the related public key certificate revocation list to said data processing apparatus, and
said data processing apparatus verifies whether or not public key certificate data of said data providing apparatus providing said distributed content data is invalid based on said public key certificate revocation list distributed from said management apparatus and controls the usage of said distributed content data based on the result of the related verification.

156. A data providing system as set forth in claim 155, wherein said management apparatus directly distributes said public key certificate revocation list to said data processing apparatus.

157. A data providing system as set forth in claim 155, wherein said management apparatus distributes said public key certificate revocation list to said data processing apparatus through said data distribution apparatus, by broadcasting, or by an on-demand system.

158. A data providing system comprising a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus, wherein:

said management apparatus manages the operation of a data providing service by said data providing apparatus, said data distribution apparatus, and said data processing apparatus, generates signature data indicating that the related data is generated by an apparatus itself by using its own secret key data when said data providing apparatus supplies data to another apparatus, generates and manages public key certificate data of public key data corresponding to secret key data of said data providing apparatus for when another apparatus verifies the legitimacy of the related signature data by using the public key data corresponding to said secret key data, generates public key certificate revocation list for specifying public key certificate data to be invalidated among said generated public key certificate data, distributes the related public key certificate revocation list to said data distribution apparatus, and
said data distribution apparatus verifies whether or not public key certificate data of said data providing apparatus providing said provided content data is invalid based on said public key certificate revocation list distributed from said management apparatus, and controls the distribution of said provided content data to said data processing apparatus based on the result of the related verification.

159. A data providing system comprising a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus, wherein:

said management apparatus manages the operation of a data providing service by said data providing apparatus, said data distribution apparatus, and said data processing apparatus, generates signature data indicating that the related data is generated by an apparatus itself by using its own secret key data when said data distribution apparatus supplies data to another apparatus, generates and manages public key

certificate data of public key data corresponding to secret key data of said data distribution apparatus for when another apparatus verifies the legitimacy of the related signature data by using the public key data corresponding to said secret key data, generates public key certificate revocation list for specifying public key certificate data to be invalidated among said generated public key certificate data, and distributes the related public key certificate revocation list to said data providing apparatus,
said data providing apparatus verifies whether or not public key certificate data of the data distribution apparatus of the destination of provision of the content data is invalid and controls the provision of said content data to said data distribution apparatus based on the result of the related verification,
said data distribution apparatus distributes said provided content data to said data processing apparatus, and
said data processing apparatus uses said distributed content data.

160. A data providing system comprising a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus, wherein:

said management apparatus manages the operation of a data providing service by said data providing apparatus, said data distribution apparatus, and said data processing apparatus, generates signature data indicating that the related data is generated by an apparatus itself by using its own secret key data when said data distribution apparatus supplies data to another apparatus, generates and manages public key certificate data of public key data corresponding to secret key data of said data distribution apparatus for when another apparatus verifies the legitimacy of the related signature data by using the public key data corresponding to said secret key data, generates public key certificate revocation list for specifying public key certificate data to be invalidated among said generated public key certificate data, and distributes the related public key certificate revocation list to said data distribution apparatus,
said data providing apparatus provides content data to said data distribution apparatus,
said data distribution apparatus distributes said provided content data and said distributed public key certificate revocation list to said data processing apparatus, and
said data processing apparatus verifies whether or not public key certificate data of said data distribution apparatus distributing said distributed content data is invalid based on said distributed public key certificate revocation list and controls the usage of said distributed content data based on the result of the related verification.

161. A data providing system as set forth in claim 160, wherein said data distribution apparatus has a configuration which makes it difficult to tamper with said public key certificate revocation list distributed from said management apparatus.

162. A data providing system as set forth in claim 160, wherein

said management apparatus encrypts said public key certificate revocation list using distribution key data and distributes it to said data distribution apparatus and distributes said distribution key data to said data processing apparatus and
said data processing apparatus decrypts said distributed public key certificate revocation list using said distribution key data.

163. A data providing system as set forth in claim 160, wherein said data distribution apparatus distributes said public key certificate revocation list to said data processing apparatus by broadcasting or by an on-demand system.

164. A data providing system comprising a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus, wherein:

said management apparatus manages the operation of a data providing service by said data providing apparatus, said data distribution apparatus, and said data processing apparatus, generates signature data indicating that the related data is generated by an apparatus itself by using its own secret key data when said data distribution apparatus supplies data to another apparatus, generates and manages public key certificate data of public key data corresponding to secret key data of said data distribution apparatus for when another apparatus verifies the legitimacy of the related signature data by using public key data corresponding to said secret key data, generates public key certificate revocation list for specifying public key certificate data to be invalidated among said generated public key certificate data, and distributes the related public key certificate revocation list to said data processing apparatus,
said data providing apparatus provides content data to said data distribution apparatus,

said data distribution apparatus distributes said provided content data to said data processing apparatus, and
said data processing apparatus verifies whether or not public key certificate data of said data distribution apparatus distributing said distributed content data is invalid based on said distributed public key certificate revocation list and controls the usage of said distributed content data based on the result of the related verification.

165. A data providing system comprising a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus, wherein:

said management apparatus manages the operation of a data providing service by said data providing apparatus, said data distribution apparatus, and said data processing apparatus, generates signature data indicating that the related data is generated by an apparatus itself by using its own secret key data when said data distribution apparatus supplies data to another apparatus, generates and manages public key certificate data of public key data corresponding to secret key data of said data distribution apparatus for when another apparatus verifies the legitimacy of the related signature data by using public key data corresponding to said secret key data, generates public key certificate revocation list for specifying public key certificate data to be invalidated among said generated public key certificate data, and distributes the related public key certificate revocation list to said data providing apparatus,
said data providing apparatus provides content data and said public key certificate revocation list to said data distribution apparatus,
said data distribution apparatus distributes said provided content data and public key certificate revocation list to said data processing apparatus, and
said data processing apparatus verifies whether or not public key certificate data of said data distribution apparatus distributing said distributed content data is invalid based on said distributed public key certificate revocation list and controls the usage of said distributed content data based on the result of the related verification.

166. A data providing system comprising a data providing apparatus, data distribution apparatus, a plurality of data processing apparatuses, and a management apparatus, wherein:

said management apparatus manages the operation of a data providing service by said data providing apparatus, said data distribution apparatus, and said data processing apparatuses, generates signature data indicating that the related data is generated by an apparatus itself by using its own secret key data when a data processing apparatus supplies data to another apparatus, generates and manages public key certificate data of public key data corresponding to secret key data of said data processing apparatuses for when another apparatus verifies the legitimacy of the related signature data by using the public key data corresponding to said secret key data, generates public key certificate revocation list for specifying public key certificate data to be invalidated among said generated public key certificate data, and distributes the related public key certificate revocation list to said data providing apparatus,
said data providing apparatus provides content data and said public key certificate revocation list to said data distribution apparatus,
said data distribution apparatus distributes said provided content data and public key certificate revocation list to said data processing apparatuses, and
said data processing apparatuses verify whether or not public key certificate data of said other data processing apparatuses are invalid based on the public key certificate revocation list distributed from said data distribution apparatus and control the communication with other data processing apparatuses based on the result of the related verification.

167. A data providing system as set forth in claim 166, wherein said data distribution apparatus has a configuration which makes it difficult to tamper with said public key certificate revocation list distributed from said management apparatus.

168. A data providing system as set forth in claim 166, wherein

said management apparatus encrypts said public key certificate revocation list using distribution key data and distributes it to said data distribution apparatus and distributes said distribution key data to said data processing apparatus and
said data processing apparatus decrypts said distributed public key certificate revocation list using said distribution key data.

169. A data providing system comprising a data providing apparatus, data distribution apparatus, a plurality of data processing apparatuses, and a manage-

ment apparatus, wherein:

said management apparatus manages the operation of a data providing service by said data providing apparatus, said data distribution apparatus, and said data processing apparatuses, generates signature data indicating that the related data is generated by an apparatus itself by using its own secret key data when a data processing apparatus supplies data to another apparatus, generates and manages public key certificate data of public key data corresponding to secret key data of said data processing apparatuses for when another apparatus verifies the legitimacy of the related signature data by using the public key data corresponding to said secret key data, generates public key certificate revocation list for specifying public key certificate data to be invalidated among said generated public key certificate data, and distributes the related public key certificate revocation list to said data providing apparatus,
said data providing apparatus provides content data to said data distribution apparatus,
said data distribution apparatus distributes said provided content data and said distributed public key certificate revocation list to said data processing apparatuses, and
said data processing apparatuses verify whether or not public key certificate data of other data processing apparatuses are invalid based on the public key certificate revocation list distributed from said data distribution apparatus, and control the communication with other data processing apparatuses based on the result of the related verification.

170. A data providing system as set forth in claim 169, wherein said data distribution apparatus has a configuration which makes it difficult to tamper with said public key certificate revocation list distributed from said management apparatus.

171. A data providing system as set forth in claim 169, wherein

said management apparatus encrypts said public key certificate revocation list using distribution key data and distributes it to said data distribution apparatus and distributes said distribution key data to said data processing apparatus and
said data processing apparatus decrypts said distributed public key certificate revocation list using said distribution key data.

172. A data providing system comprising a data providing apparatus, data distribution apparatus, a plurality of data processing apparatuses, and a management apparatus, wherein:

a data processing apparatus supplies registration data, indicating an already registered data processing apparatus connected in a predetermined network to which is connected, to said management apparatus, refers to a revocation flag in registration data supplied from said management apparatus and restricts communication with another data processing apparatus having public key certificate data indicated as invalid by the revocation flag,
said management apparatus manages the operation of a data providing service by said data providing apparatus, said data distribution apparatus, and said data processing apparatuses, generates and manages public key certificate data of public key data corresponding to secret key data for when a data processing apparatus generates signature data indicating legitimacy of data using its own secret key data when supplying data to another apparatus, generates public key certificate revocation list for specifying public key certificate data to be invalidated among said generated public key certificate data, stores the related public key certificate revocation list, generates new registration data by setting said revocation flag in said registration data supplied from data processing apparatuses based on the related public key certificate revocation list, and distributes the related generated registration data to said data processing apparatuses,
said data providing apparatus provides content data to said data distribution apparatus, and
said data distribution apparatus distributes said provided content data to said data processing apparatuses.

173. A data providing system comprising a data providing apparatus, data distribution apparatus, a plurality of data processing apparatuses, and a management apparatus, wherein:

said management apparatus manages the operation of a data providing service by said data providing apparatus, said data distribution apparatus, and said data processing apparatuses, generates and manages public key certificate data of public key data corresponding to said secret key data for when a data processing apparatus generates signature data indicating the legitimacy of data by using its own secret key data when supplying the related data to another apparatus, generates public key certificate revocation list for specifying public key certificate data to be invalidated among said

generated public key certificate data, and distributes the related public key certificate revocation list to said data providing apparatus,
said data providing apparatus provides content data and said public key certificate revocation list to said data distribution apparatus,
said data distribution apparatus distributes said provided content data and said public key certificate revocation list to said data processing apparatuses, and
a data processing apparatus sets a revocation flag in registration data indicating an already registered data processing apparatus connected in a predetermined network to which it is connected based on said distributed public key certificate revocation list and restricts communication with another data processing apparatus having public key certificate data indicated as invalid by the related revocation flag.

174. A data providing system comprising a data providing apparatus, data distribution apparatus, a plurality of data processing apparatuses, and a management apparatus, wherein:

said management apparatus manages the operation of a data providing service by said data providing apparatus, said data distribution apparatus, and said data processing apparatuses, generates and manages public key certificate data of public key data corresponding to secret key data for when a data processing apparatus generates signature data indicating the legitimacy of the data by using its own secret key data when supplying the related data to another apparatus, generates public key certificate revocation list for specifying public key certificate data to be invalidated among said generated public key certificate data, and distributes the related public key certificate revocation list to said data distribution apparatus,
said data providing apparatus provides content data to said data distribution apparatus,
said data distribution apparatus distributes said provided content data and said public key certificate revocation list to said data processing apparatuses, and
a data processing apparatus sets a revocation flag in registration data indicating an already registered data processing apparatus connected in a predetermined network to which it is connected based on said distributed public key certificate revocation list and restricts communication with another data processing apparatus having public key certificate data indicated as invalid by the related revocation flag.

175. A data providing system comprising a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus, wherein:

said data providing apparatus provides content data and usage control policy data indicating the handling of the related content data to said data distribution apparatus,
said data distribution apparatus distributes said provided content data and said usage control policy data to said data processing apparatus,
said data processing apparatus has a first module for communicating with said data distribution apparatus and a second module for determining at least one of a purchase mode and usage mode of said distributed content data based on said distributed usage control policy data and transmitting log data indicating the log of the related determined purchase mode and usage mode to said management apparatus,
said management apparatus manages the data providing apparatus, data distribution apparatus, and data processing apparatus and
has a settlement function for performing profit distribution processing for distributing the profit obtained accompanied with said data processing apparatus receiving distribution of said content data and purchasing and using said content data to related parties of said data providing apparatus and said data distribution apparatus based on said log data received from said second module and performing settlement based on the result of the related profit distribution processing and a right management function for registering said usage control policy data.

176. A data providing system as set forth in claim 175, wherein said management apparatus has

a first management apparatus having a settlement function and
a second management apparatus having a right management function.

177. A data providing system as set forth in claim 175, wherein said settlement is electronic settlement.

178. A data providing system comprising a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus, wherein:

said data providing apparatus provides content data and usage control policy data indicating the handling of the related content data to said data distribution apparatus,
said data distribution apparatus has a charging

function for performing settlement processing by using settlement claim data distributed from said management apparatus and distributes said provided content data and said usage control policy data to said data processing apparatus,
said data processing apparatus has a first module for communicating with said data distribution apparatus and a second module for determining at least one of a purchase mode and usage mode of said distributed content data based on said distributed usage control policy data and transmitting log data indicating the log of the related determined purchase mode and usage mode to said management apparatus,
said management apparatus manages the data providing apparatus, data distribution apparatus, and data processing apparatus and
has a settlement claim data creation function for performing profit distribution processing for distributing the profit obtained accompanied with said data processing apparatus receiving distribution of said content data and purchasing and using said content data to related parties of said data providing apparatus and said data distribution apparatus based on said log data received from said second module, creating settlement claim data used when performing settlement based on the result of the related profit distribution processing, and supplying the same to said data distribution apparatus and a right management function for registering said usage control policy data.

179. A data providing system comprising a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus, wherein:

said data providing apparatus has a charging function for performing settlement processing by using settlement claim data distributed from said management apparatus and provides content data and usage control policy data indicating the handling of the related content data to said data distribution apparatus,
said data distribution apparatus distributes said provided content data and said usage control policy data to said data processing apparatus,
said data processing apparatus has a first module for communicating with said data distribution apparatus and a second module for determining at least one of a purchase mode and usage mode of said distributed content data based on said distributed usage control policy data and transmitting log data indicating the log of the related determined purchase mode and usage mode to said management apparatus,
said management apparatus manages the data providing apparatus, data distribution apparatus, and data processing apparatus and
has a settlement claim data creation function for performing profit distribution processing for distributing the profit obtained accompanied with said data processing apparatus receiving said distribution of said content data and purchasing and using said content data to related parties of said data providing apparatus and said data distribution apparatus based on said log data received from said second module, creating settlement claim data used when performing settlement based on the result of the related profit distribution processing, and distributing the same to said data providing apparatus and a right management function for registering said usage control policy data.

180. A data providing method using a data providing apparatus, data processing apparatus, and management apparatus comprising the steps of

distributing content data and usage control policy data indicating the handling of the related content data from said data providing apparatus to said data processing apparatus,
determining at least one of the purchase mode and the usage mode of said distributed content data based on said distributed usage control policy data and transmitting log data indicating the log of at least one of the related determined purchase mode and usage mode to said management apparatus at said data processing apparatus, and
performing profit distribution processing for distributing the profit obtained accompanied with said purchase and said usage of said content data in said data processing apparatus to related parties of said data providing apparatus based on said received log data at said management apparatus.

181. A data providing method using a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus comprising the steps of:

providing content data and usage control policy data indicating the handling of the related content data from said data providing apparatus to said data distribution apparatus,
distributing said provided content data and said usage control policy data from said data distribution apparatus to said data processing apparatus,
determining at least one of the purchase mode and the usage mode of said distributed content

data based on said distributed usage control policy data and transmitting log data indicating the log of the related determined purchase mode and usage mode to said management apparatus at said data processing apparatus, and

performing profit distribution processing for distributing the profit obtained accompanied with said data processing apparatus receiving said distribution of said content data and purchasing and using said content data to related parties of said data providing apparatus and said data distribution apparatus based on said log data received from said second module at said management apparatus.

182. A data providing method using a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus comprising the steps of:

providing content data and usage control policy data indicating the handling of the related content data from said data providing apparatus to said data distribution apparatus,

distributing said content data and said usage control policy data provided from said data distribution apparatus to said data processing apparatus to said data processing apparatus,

generating data distribution apparatus use purchase log data indicating the log of the purchase of said content data distributed from said data distribution apparatus and transmitting the same to said data distribution apparatus, determining at least one of a purchase mode and usage mode of said distributed content data based on said distributed usage control policy data, and transmitting management apparatus use log data indicating the log of the related determined purchase mode and usage mode to said management apparatus at said data processing apparatus,

distributing the profit obtained accompanied with said purchase and said usage of said content data in said data processing apparatus to related parties of said data providing apparatus and said data distribution apparatus based on said management apparatus use log data at said management apparatus, and

performing charging processing concerning the distribution of said content data based on the data distribution apparatus use purchase log data received from said data processing apparatus at said data distribution apparatus.

183. A data providing method using a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus to provide content data, wherein

said data providing apparatus provides content data to said data distribution apparatus,

said data distribution apparatus distributes said provided content data to said data processing apparatus, and

said data processing apparatus manages the operation of a data provision service by said data providing apparatus, data distribution apparatus, and data processing apparatus, and

said management apparatus manages operation of a data providing service by said data providing apparatus, said data distribution apparatus, and said data processing apparatus, wherein

the transmission of data among said data providing apparatus, said data distribution apparatus, said data processing apparatus, and said management apparatus is carried out by using mutual authentication using a public key encryption method, signature creation, signature verification, and encryption of data by a common key encryption method.

184. A data providing method using a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus to provide content data, wherein

said data providing apparatus provides content data to said data distribution apparatus,

said data distribution apparatus distributes said provided content data to said data processing apparatus,

said data processing apparatus uses said distributed content data, and

said management apparatus manages the operation of a data providing service by said data providing apparatus, said data distribution apparatus, and said data processing apparatus, generates signature data indicating that the related data is generated by itself by using its own secret key data when each of said data providing apparatus, said data distribution apparatus, and said data processing apparatus supplies the data to another apparatus, and generates and manages public key certificate data of public key data corresponding to secret key data of said data providing apparatus, said data distribution apparatus, and said data processing apparatus when the legitimacy of the signature data corresponding to the data is verified by using the public key data of the related other apparatus when receiving the supply of the related data from the other apparatus, wherein

said data providing apparatus, said data distribution apparatus, and said data processing ap-

paratus acquire said their own public key certificate data from said management apparatus before communicating with the other apparatus and transmit the related acquired public key certificate data to said other apparatus.

185. A data providing method using a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus to provide content data, wherein

said data providing apparatus provides content data to said data distribution apparatus,
said data distribution apparatus distributes said provided content data to said data processing apparatus,
said data processing apparatus uses said distributed content data, and
said management apparatus manages the operation of a data providing service by said data providing apparatus, said data distribution apparatus, and said data processing apparatus, generates the signature data indicating that the related data is generated by itself by using its own secret key data when each of said data providing apparatus, said data distribution apparatus, and said data processing apparatus supplies data to another apparatus, and generates and manages public key certificate data of public key data corresponding to secret key data of said data providing apparatus, said data distribution apparatus, and said data processing apparatus when the legitimacy of the signature data corresponding to the data is verified by using the public key data of the related other apparatus when receiving the supply of the related data from the other apparatus, wherein
said data providing apparatus, said data distribution apparatus, and said data processing apparatus acquire their own public key certificate data from said management apparatus when communicating with the other apparatus and transmit the related acquired public key certificate data to said other apparatus at said communication.

186. A data providing method using a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus to provide content data, wherein:

said data providing apparatus provides content data to said data distribution apparatus,
said data distribution apparatus distributes said provided content data to said data processing apparatus,
said data processing apparatus uses said distributed content data, and
said management apparatus manages the operation of a data providing service by said data providing apparatus, said data distribution apparatus, and said data processing apparatus, generates signature data indicating that the related data is generated by itself by using its own secret key data when each of said data providing apparatus, said data distribution apparatus, and said data processing apparatus supplies data to another apparatus, generates and manages public key certificate data of public key data corresponding to secret key data of said data providing apparatus, said data distribution apparatus, and said data processing apparatus when the legitimacy of the signature data corresponding to the data is verified by using the public key data of the related other apparatus when receiving the supply of the related data from the other apparatus, and generates public key certificate revocation list for specifying public key certificate data to be invalidated among said generated public key certificate data and thereby to restrict said communication or said distribution using public key certificate data specified by said public key certificate revocation list by said data providing apparatus, said data distribution apparatus, and said data processing apparatus.

187. A data providing method as set forth in claim 186, wherein said management apparatus generates public key certificate revocation list specifying public key certificate data corresponding to said data providing apparatus, said data distribution apparatus, and said data processing apparatus used for illegal actions.

188. A data providing method using a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus to provide content data, wherein:

said data providing apparatus provides content data to said data distribution apparatus,
said data distribution apparatus distributes said provided content data to said data processing apparatus,
said management apparatus manages the operation of a data providing service by said data providing apparatus, said data distribution apparatus, and said data processing apparatus, generates signature data indicating that the related data is generated by an apparatus itself by using its own secret key data when said data providing apparatus supplies data to another apparatus, generates and manages public key certificate data of public key data corresponding to secret key data of said data providing ap-

paratus for when another apparatus verifies the legitimacy of the related signature data by using the public key data corresponding to said secret key data, generates public key certificate revocation list for specifying public key certificate data to be invalidated among said generated public key certificate data, distributes the related public key certificate revocation list to said data processing apparatus, and
said data processing apparatus verifies whether or not public key certificate data of said data providing apparatus providing said distributed content data is invalid based on said public key certificate revocation list distributed from said management apparatus and controls the usage of said distributed content data based on the result of the related verification.

189. A data providing method as set forth in claim 188, wherein said management apparatus directly distributes said public key certificate revocation list to said data processing apparatus.

190. A data providing method as set forth in claim 188, wherein said management apparatus distributes said public key certificate revocation list to said data processing apparatus through said data distribution apparatus, by broadcasting, or by an on-demand system.

191. A data providing method using a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus to provide content data, wherein:

said management apparatus manages the operation of a data providing service by said data providing apparatus, said data distribution apparatus, and said data processing apparatus, generates signature data indicating that the related data is generated by an apparatus itself by using its own secret key data when said data providing apparatus supplies data to another apparatus, generates and manages public key certificate data of public key data corresponding to secret key data of said data providing apparatus for when another apparatus verifies the legitimacy of the related signature data by using the public key data corresponding to said secret key data, generates public key certificate revocation list for specifying public key certificate data to be invalidated among said generated public key certificate data, distributes the related public key certificate revocation list to said data distribution apparatus, and
said data distribution apparatus verifies whether or not public key certificate data of said data providing apparatus providing said provided content data is invalid based on said public key certificate revocation list distributed from said management apparatus, and controls the distribution of said provided content data to said data processing apparatus based on the result of the related verification.

192. A data providing method using a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus to provide content data, wherein:

said management apparatus manages the operation of a data providing service by said data providing apparatus, said data distribution apparatus, and said data processing apparatus, generates signature data indicating that the related data is generated by an apparatus itself by using its own secret key data when said data distribution apparatus supplies data to another apparatus, generates and manages public key certificate data of public key data corresponding to secret key data of said data distribution apparatus for when another apparatus verifies the legitimacy of the related signature data by using the public key data corresponding to said secret key data, generates public key certificate revocation list for specifying public key certificate data to be invalidated among said generated public key certificate data, and distributes the related public key certificate revocation list to said data providing apparatus,
said data providing apparatus verifies whether or not public key certificate data of the data distribution apparatus of the destination of provision of the content data is invalid and controls the provision of said content data to said data distribution apparatus based on the result of the related verification,
said data distribution apparatus distributes said provided content data to said data processing apparatus, and
said data processing apparatus uses said distributed content data.

193. A data providing method using a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus to provide content data, wherein:

said management apparatus manages the operation of a data providing service by said data providing apparatus, said data distribution apparatus, and said data processing apparatus, generates signature data indicating that the related data is generated by an apparatus itself by using its own secret key data when said data distribution apparatus supplies data to another apparatus, generates and manages public key certificate data of public

key data corresponding to secret key data of said data distribution apparatus for when another apparatus verifies the legitimacy of the related signature data by using the public key data corresponding to said secret key data, generates public key certificate revocation list for specifying public key certificate data to be invalidated among said generated public key certificate data, and distributes the related public key certificate revocation list to said data distribution apparatus,

said data providing apparatus provides content data to said data distribution apparatus,
said data distribution apparatus distributes said provided content data and said distributed public key certificate revocation list to said data processing apparatus, and
said data processing apparatus verifies whether or not public key certificate data of said data distribution apparatus distributing said distributed content data is invalid based on said distributed public key certificate revocation list and controls the usage of said distributed content data based on the result of the related verification.

194. A data providing method as set forth in claim 193, wherein said data distribution apparatus has a configuration which makes it difficult to tamper with said public key certificate revocation list distributed from said management apparatus.

195. A data providing method as set forth in claim 193, wherein

said management apparatus encrypts said public key certificate revocation list using distribution key data and distributes it to said data distribution apparatus and distributes said distribution key data to said data processing apparatus and
said data processing apparatus decrypts said distributed public key certificate revocation list using said distribution key data.

196. A data providing method as set forth in claim 160, wherein said data distribution apparatus distributes said public key certificate revocation list to said data processing apparatus by broadcasting or by an on-demand system.

197. A data providing method using a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus to provide content data, wherein:

said management apparatus manages the operation of a data providing service by said data providing apparatus, said data distribution apparatus, and said data processing apparatus, generates signature data indicating that the related data is generated by an apparatus itself by using its own secret key data when said data distribution apparatus supplies data to another apparatus, generates and manages public key certificate data of public key data corresponding to secret key data of said data distribution apparatus for when another apparatus verifies the legitimacy of the related signature data by using public key data corresponding to said secret key data, generates public key certificate revocation list for specifying public key certificate data to be invalidated among said generated public key certificate data, and distributes the related public key certificate revocation list to said data processing apparatus,
said data providing apparatus provides content data to said data distribution apparatus,
said data distribution apparatus distributes said provided content data to said data processing apparatus, and
said data processing apparatus verifies whether or not public key certificate data of said data distribution apparatus distributing said distributed content data is invalid based on said distributed public key certificate revocation list and controls the usage of said distributed content data based on the result of the related verification.

198. A data providing method using a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus to provide content data, wherein:

said management apparatus manages the operation of a data providing service by said data providing apparatus, said data distribution apparatus, and said data processing apparatus, generates signature data indicating that the related data is generated by an apparatus itself by using its own secret key data when said data distribution apparatus supplies data to another apparatus, generates and manages public key certificate data of public key data corresponding to secret key data of said data distribution apparatus for when another apparatus verifies the legitimacy of the related signature data by using public key data corresponding to said secret key data, generates public key certificate revocation list for specifying public key certificate data to be invalidated among said generated public key certificate data, and distributes the related public key certificate revocation list to said data providing apparatus,
said data providing apparatus provides content

data and said public key certificate revocation list to said data distribution apparatus,
said data distribution apparatus distributes said provided content data and public key certificate revocation list to said data processing apparatus, and
said data processing apparatus verifies whether or not public key certificate data of said data distribution apparatus distributing said distributed content data is invalid based on said distributed public key certificate revocation list and controls the usage of said distributed content data based on the result of the related verification.

199. A data providing method using a data providing apparatus, data distribution apparatus, a plurality of data processing apparatuses, and a management apparatus to provide content data, wherein:

said management apparatus manages the operation of a data providing service by said data providing apparatus, said data distribution apparatus, and said data processing apparatuses, generates signature data indicating that the related data is generated by an apparatus itself by using its own secret key data when a data processing apparatus supplies data to another apparatus, generates and manages public key certificate data of public key data corresponding to secret key data of said data processing apparatuses for when another apparatus verifies the legitimacy of the related signature data by using the public key data corresponding to said secret key data, generates public key certificate revocation list for specifying public key certificate data to be invalidated among said generated public key certificate data, and distributes the related public key certificate revocation list to said data providing apparatus,
said data providing apparatus provides content data and said public key certificate revocation list to said data distribution apparatus,
said data distribution apparatus distributes said provided content data and public key certificate revocation list to said data processing apparatuses, and
said data processing apparatuses verify whether or not public key certificate data of said other data processing apparatuses are invalid based on the public key certificate revocation list distributed from said data distribution apparatus and control the communication with other data processing apparatuses based on the result of the related verification.

200. A data providing method as set forth in claim 199, wherein said data distribution apparatus has a configuration which makes it difficult to tamper with said public key certificate revocation list distributed from said management apparatus.

201. A data providing method as set forth in claim 199, wherein

said management apparatus encrypts said public key certificate revocation list using distribution key data and distributes it to said data distribution apparatus and distributes said distribution key data to said data processing apparatus and
said data processing apparatus decrypts said distributed public key certificate revocation list using said distribution key data.

202. A data providing method using a data providing apparatus, data distribution apparatus, a plurality of data processing apparatuses, and a management apparatus to provide content data, wherein:

said management apparatus manages the operation of a data providing service by said data providing apparatus, said data distribution apparatus, and said data processing apparatuses, generates signature data indicating that the related data is generated by an apparatus itself by using its own secret key data when a data processing apparatus supplies data to another apparatus, generates and manages public key certificate data of public key data corresponding to secret key data of said data processing apparatuses for when another apparatus verifies the legitimacy of the related signature data by using the public key data corresponding to said secret key data, generates public key certificate revocation list for specifying public key certificate data to be invalidated among said generated public key certificate data, and distributes the related public key certificate revocation list to said data providing apparatus,
said data providing apparatus provides content data to said data distribution apparatus,
said data distribution apparatus distributes said provided content data and said distributed public key certificate revocation list to said data processing apparatuses, and
said data processing apparatuses verify whether or not public key certificate data of other data processing apparatuses are invalid based on the public key certificate revocation list distributed from said data distribution apparatus, and control the communication with other data processing apparatuses based on the result of the related verification.

203. A data providing method as set forth in claim 202,

wherein said data distribution apparatus has a configuration which makes it difficult to tamper with said public key certificate revocation list distributed from said management apparatus.

204. A data providing method as set forth in claim 202, wherein

said management apparatus encrypts said public key certificate revocation list using distribution key data and distributes it to said data distribution apparatus and distributes said distribution key data to said data processing apparatus and
said data processing apparatus decrypts said distributed public key certificate revocation list using said distribution key data.

205. A data providing method using a data providing apparatus, data distribution apparatus, a plurality of data processing apparatuses, and a management apparatus to provide content data, wherein:

a data processing apparatus supplies registration data, indicating an already registered data processing apparatus connected in a predetermined network to which is connected, to said management apparatus, refers to a revocation flag in registration data supplied from said management apparatus and restricts communication with another data processing apparatus having public key certificate data indicated as invalid by the revocation flag,
said management apparatus manages the operation of a data providing service by said data providing apparatus, said data distribution apparatus, and said data processing apparatuses, generates and manages public key certificate data of public key data corresponding to secret key data for when a data processing apparatus generates signature data indicating legitimacy of data using its own secret key data when supplying data to another apparatus, generates public key certificate revocation list for specifying public key certificate data to be invalidated among said generated public key certificate data, stores the related public key certificate revocation list, generates new registration data by setting said revocation flag in said registration data supplied from data processing apparatuses based on the related public key certificate revocation list, and distributes the related generated registration data to said data processing apparatuses,
said data providing apparatus provides content data to said data distribution apparatus, and
said data distribution apparatus distributes said provided content data to said data processing apparatuses.

206. A data providing method using a data providing apparatus, data distribution apparatus, a plurality of data processing apparatuses, and a management apparatus to provide content data, wherein:

said management apparatus manages the operation of a data providing service by said data providing apparatus, said data distribution apparatus, and said data processing apparatuses, generates and manages public key certificate data of public key data corresponding to said secret key data for when a data processing apparatus generates signature data indicating the legitimacy of data by using its own secret key data when supplying the related data to another apparatus, generates public key certificate revocation list for specifying public key certificate data to be invalidated among said generated public key certificate data, and distributes the related public key certificate revocation list to said data providing apparatus,
said data providing apparatus provides content data and said public key certificate revocation list to said data distribution apparatus,
said data distribution apparatus distributes said provided content data and said public key certificate revocation list to said data processing apparatuses, and
a data processing apparatus sets a revocation flag in registration data indicating an already registered data processing apparatus connected in a predetermined network to which it is connected based on said distributed public key certificate revocation list and restricts communication with another data processing apparatus having public key certificate data indicated as invalid by the related revocation flag.

207. A data providing method using a data providing apparatus, data distribution apparatus, a plurality of data processing apparatuses, and a management apparatus to provide content data, wherein:

said management apparatus manages the operation of a data providing service by said data providing apparatus, said data distribution apparatus, and said data processing apparatuses, generates and manages public key certificate data of public key data corresponding to secret key data for when a data processing apparatus generates signature data indicating the legitimacy of the data by using its own secret key data when supplying the related data to another apparatus, generates public key certificate revocation list for specifying public key certificate data to be invalidated among said

generated public key certificate data, and distributes the related public key certificate revocation list to said data distribution apparatus,
said data providing apparatus provides content data to said data distribution apparatus,
said data distribution apparatus distributes said provided content data and said public key certificate revocation list to said data processing apparatuses, and
a data processing apparatus sets a revocation flag in registration data indicating an already registered data processing apparatus connected in a predetermined network to which it is connected based on said distributed public key certificate revocation list and restricts communication with another data processing apparatus having public key certificate data indicated as invalid by the related revocation flag.

208. A data providing method using a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus to provide content data, wherein:

said data providing apparatus provides content data and usage control policy data indicating the handling of the related content data to said data distribution apparatus,
said data distribution apparatus distributes said provided content data and said usage control policy data to said data processing apparatus,
said data processing apparatus has a first module for communicating with said data distribution apparatus and a second module for determining at least one of a purchase mode and usage mode of said distributed content data based on said distributed usage control policy data and transmitting log data indicating the log of the related determined purchase mode and usage mode to said management apparatus,
said management apparatus manages the data providing apparatus, data distribution apparatus, and data processing apparatus and
has a settlement function for performing profit distribution processing for distributing the profit obtained accompanied with said data processing apparatus receiving distribution of said content data and purchasing and using said content data to related parties of said data providing apparatus and said data distribution apparatus based on said log data received from said second module and performing settlement based on the result of the related profit distribution processing and a right management function for registering said usage control policy data.

FIG.1

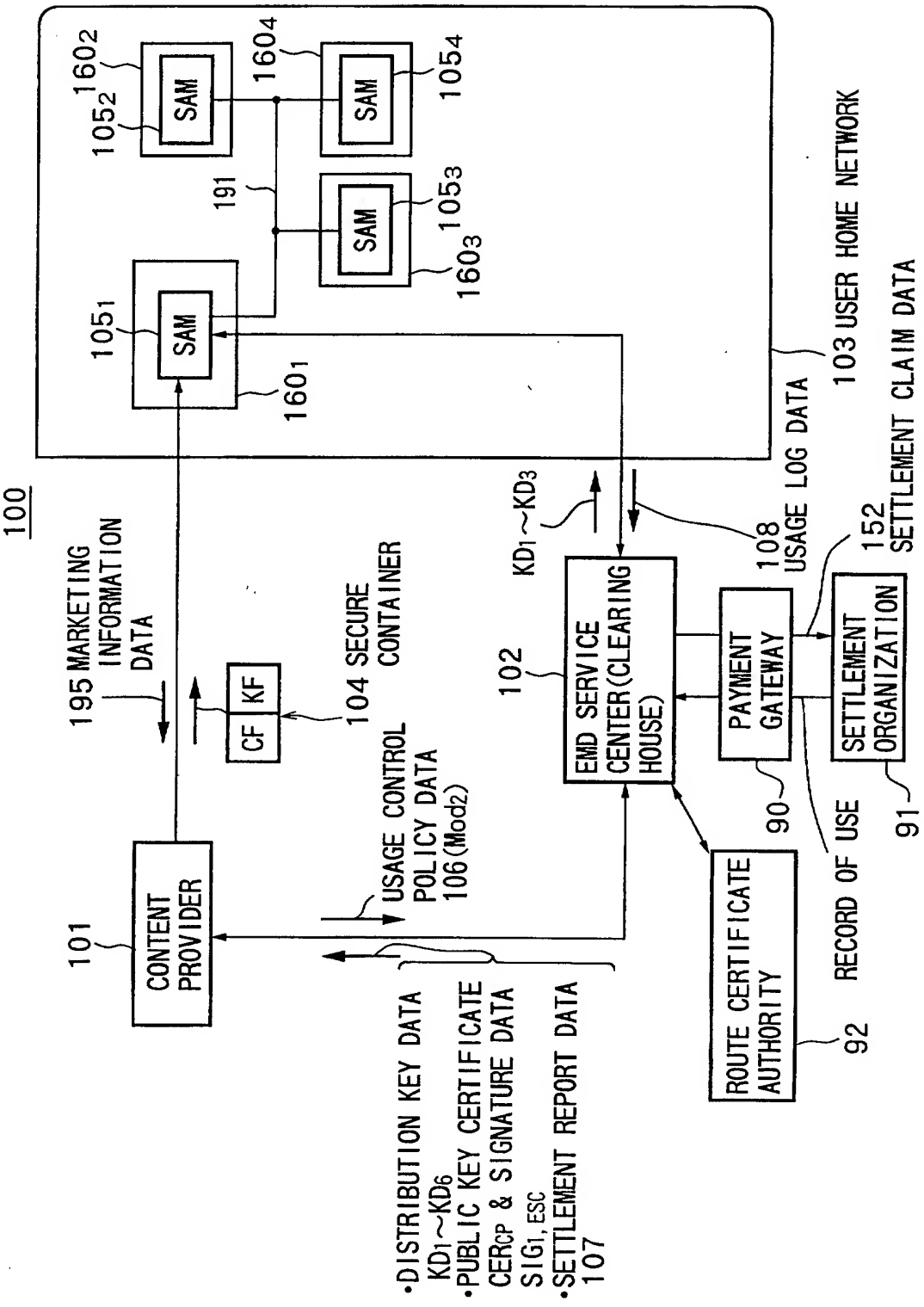

100
101 CONTENT PROVIDER
195 MARKETING INFORMATION DATA
CF KF
104 SECURE CONTAINER
USAGE CONTROL POLICY DATA 106(Mod2)
•DISTRIBUTION KEY DATA KD1~KD6
•PUBLIC KEY CERTIFICATE CERCP & SIGNATURE DATA SIG1, ESC
•SETTLEMENT REPORT DATA 107
102 EMD SERVICE CENTER(CLEARING HOUSE)
KD1~KD3
108 USAGE LOG DATA
103 USER HOME NETWORK
SAM 1051 1601
SAM 1052 1602
SAM 1053 1603
SAM 1054 1604
191
PAYMENT GATEWAY
90
SETTLEMENT ORGANIZATION
91
152 SETTLEMENT CLAIM DATA
RECORD OF USE
ROUTE CERTIFICATE AUTHORITY
92

FIG.2

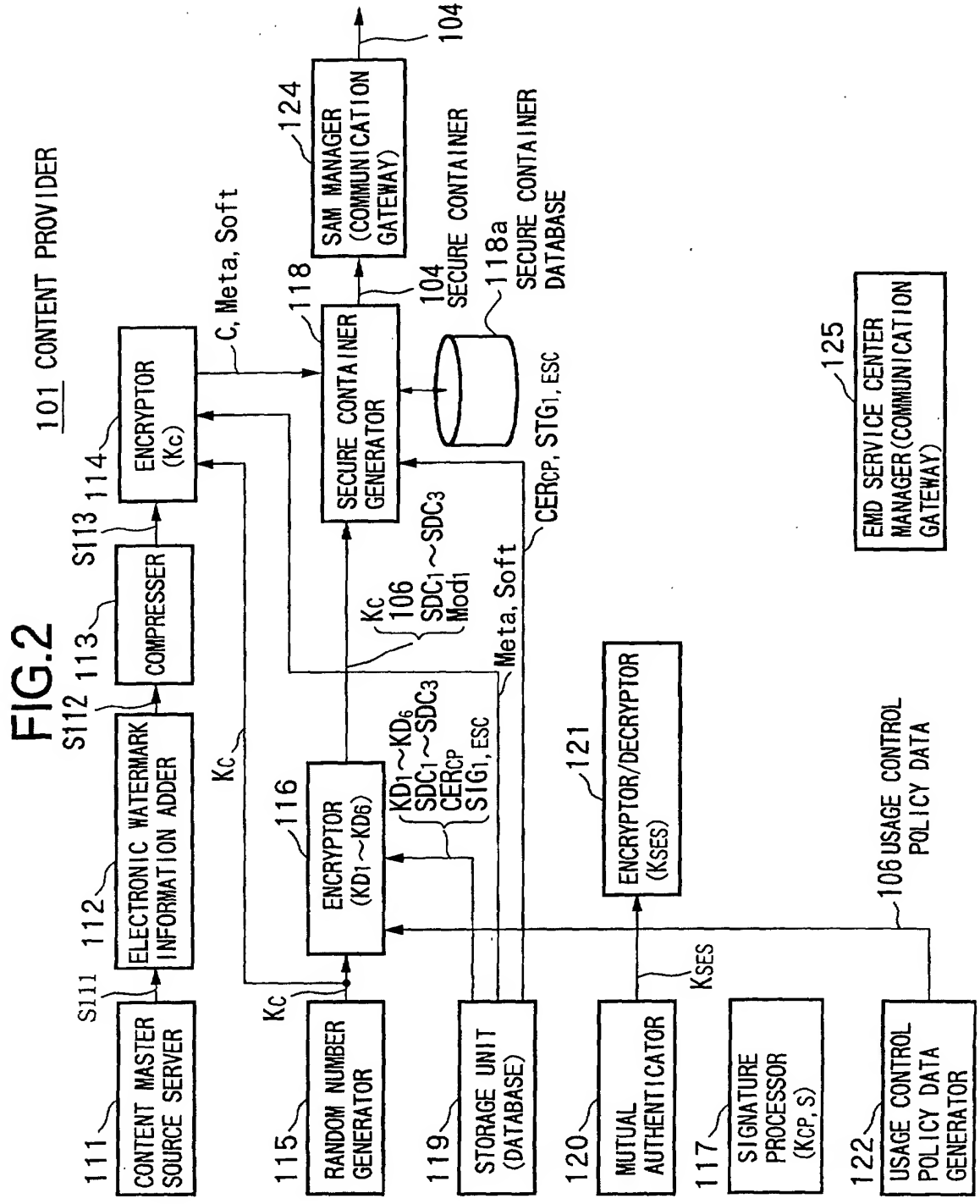
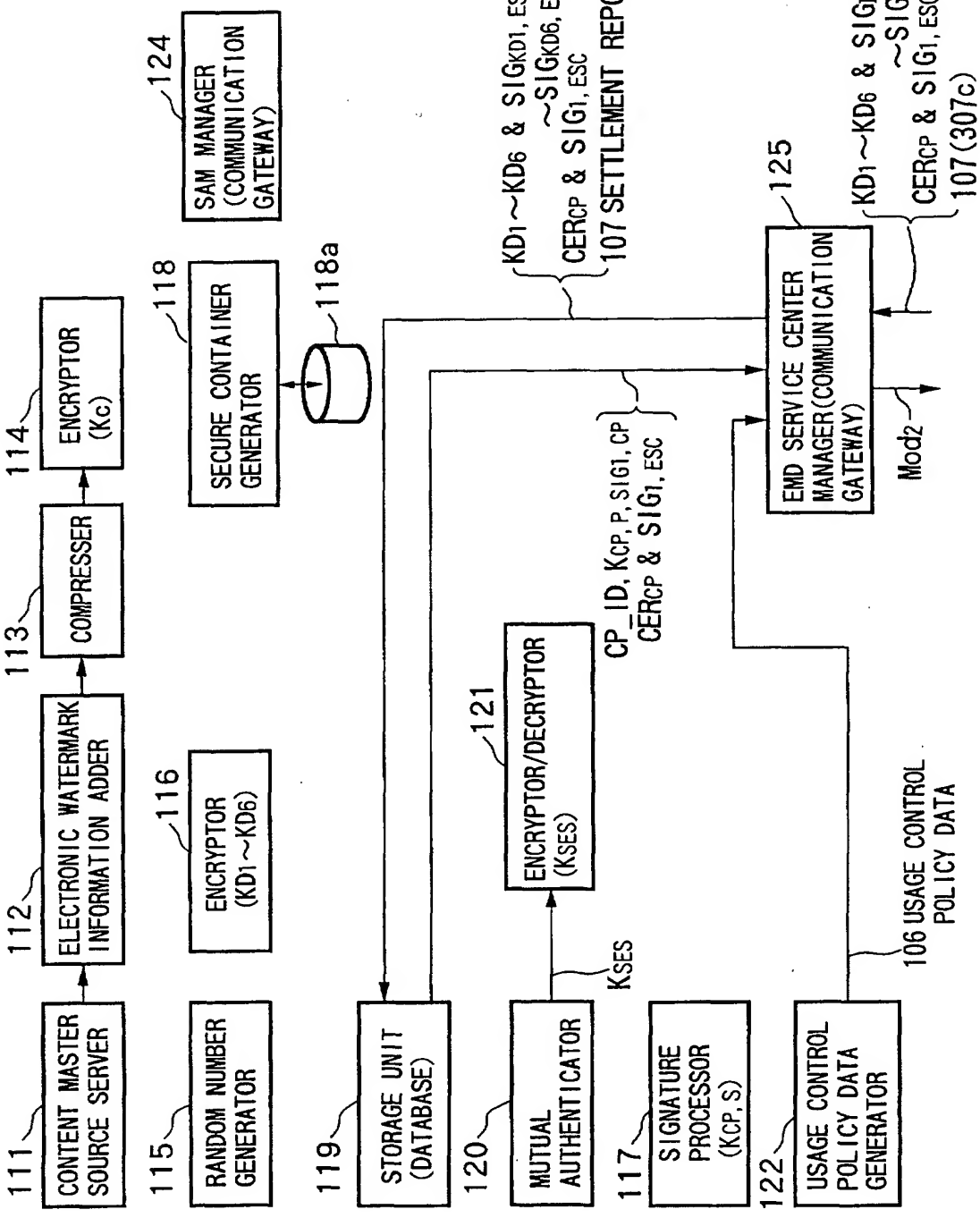

101 CONTENT PROVIDER
111 CONTENT MASTER SOURCE SERVER
S111
112 ELECTRONIC WATERMARK INFORMATION ADDER
S112
113 COMPRESSER
S113
114 ENCRYPTOR (Kc)
C, Meta, Soft
118 SECURE CONTAINER GENERATOR
124 SAM MANAGER (COMMUNICATION GATEWAY)
104
104 SECURE CONTAINER
118a SECURE CONTAINER DATABASE
125 EMD SERVICE CENTER MANAGER (COMMUNICATION GATEWAY)
Kc
116 ENCRYPTOR (KD1~KD6)
KD1~KD6
SDC1~SDC3
CERCP
SIG1, ESC
Kc 106
SDC1~SDC3
Mod1
Meta, Soft
CERCP, STG1, ESC
121 ENCRYPTOR/DECRYPTOR (KSES)
106 USAGE CONTROL POLICY DATA
KSES
115 RANDOM NUMBER GENERATOR
119 STORAGE UNIT (DATABASE)
120 MUTUAL AUTHENTICATOR
117 SIGNATURE PROCESSOR (KCP, S)
122 USAGE CONTROL POLICY DATA GENERATOR

FIG.3


101 CONTENT PROVIDER
111 CONTENT MASTER SOURCE SERVER
112 ELECTRONIC WATERMARK INFORMATION ADDER
113 COMPRESSER
114 ENCRYPTOR (Kc)
115 RANDOM NUMBER GENERATOR
116 ENCRYPTOR (KD1~KD6)
117 SIGNATURE PROCESSOR (KCP, S)
118 SECURE CONTAINER GENERATOR
118a
119 STORAGE UNIT (DATABASE)
120 MUTUAL AUTHENTICATOR
121 ENCRYPTOR/DECRYPTOR (KSES)
122 USAGE CONTROL POLICY DATA GENERATOR
124 SAM MANAGER (COMMUNICATION GATEWAY)
125 EMD SERVICE CENTER MANAGER(COMMUNICATION GATEWAY)
KSES
CP_ID, KCP, P, SIG1, CP
CERCP & SIG1, ESC
KD1~KD6 & SIGKD1, ESC
~SIGKD6, ESC
CERCP & SIG1, ESC
107 SETTLEMENT REPORT
106 USAGE CONTROL POLICY DATA
Mod2
KD1~KD6 & SIGKD1, ESC
~SIGKD6, ESC
CERCP & SIG1, ESC
107(307c)

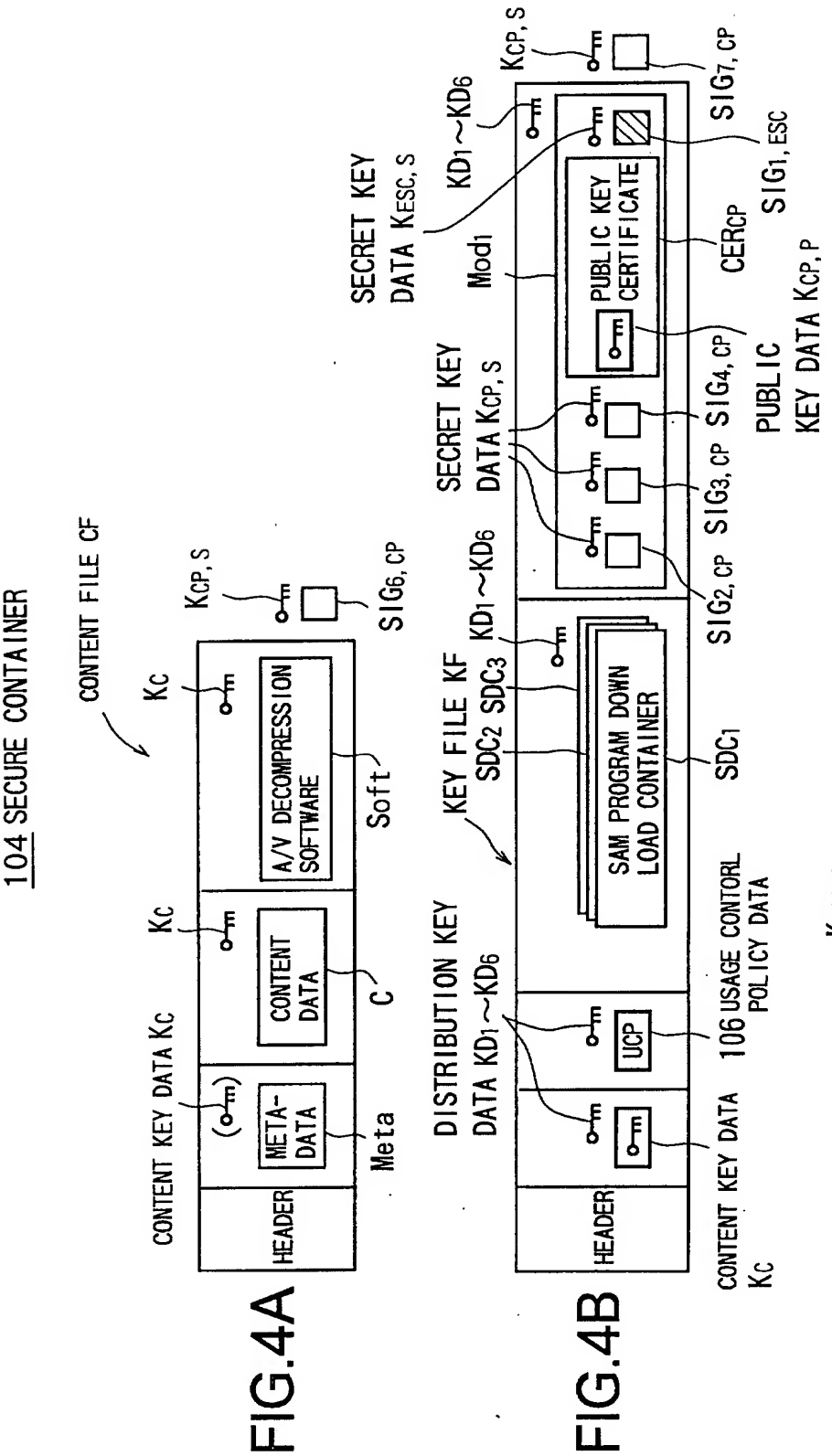

104 SECURE CONTAINER
CONTENT FILE CF
Kc
KCP, S
SIG6, CP
CONTENT KEY DATA Kc
HEADER
META-DATA
Meta
CONTENT DATA
C
A/V DECOMPRESSION SOFTWARE
Soft
FIG.4A
KEY FILE KF
SDC2 SDC3
KD1~KD6
DISTRIBUTION KEY DATA KD1~KD6
SECRET KEY DATA KCP, S
SECRET KEY DATA KESC, S
Mod1
KD1~KD6
KCP, S
SIG7, CP
PUBLIC KEY CERTIFICATE
CERCP
SIG1, ESC
SIG2, CP
SIG3, CP
SIG4, CP
PUBLIC KEY DATA KCP, P
HEADER
UCP
SAM PROGRAM DOWN LOAD CONTAINER
SDC1
106 USAGE CONTORL POLICY DATA
CONTENT KEY DATA Kc
FIG.4B
KESC, S
SIG1, ESC
SIGNATURE DATA
PUBLIC KEY CERTIFICATE
KCP, P
CERCP
FIG.4C

FIG.5

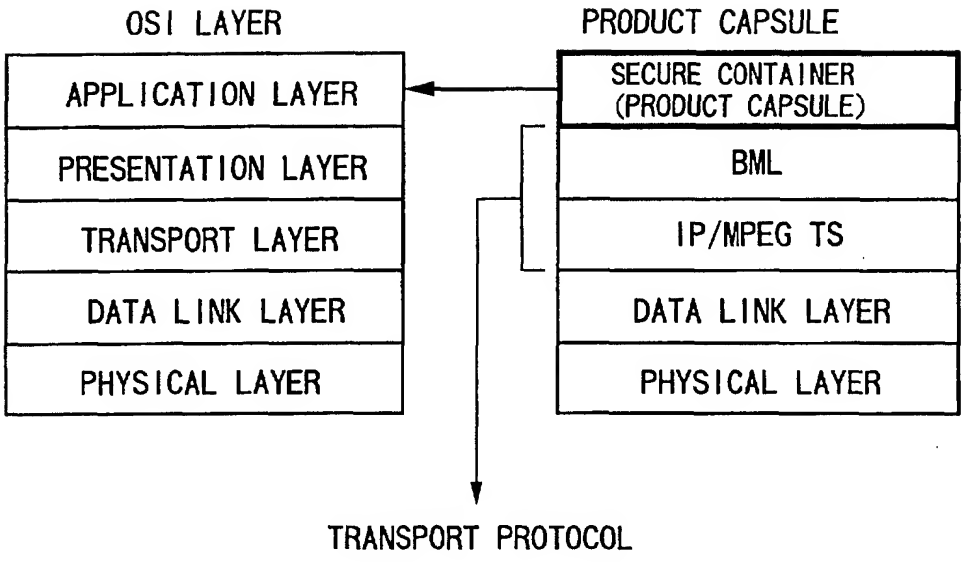
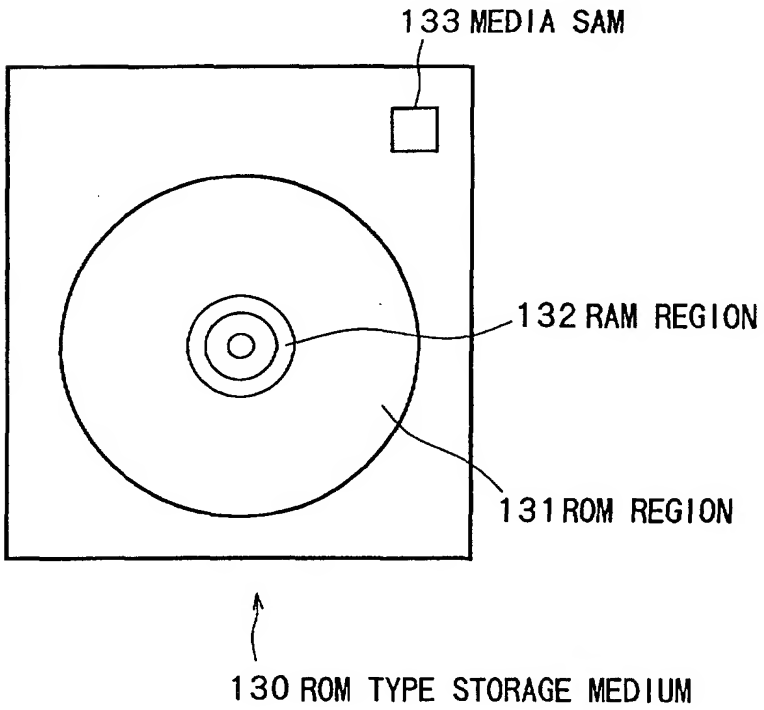

OSI LAYER
APPLICATION LAYER
PRESENTATION LAYER
TRANSPORT LAYER
DATA LINK LAYER
PHYSICAL LAYER
PRODUCT CAPSULE
SECURE CONTAINER (PRODUCT CAPSULE)
BML
IP/MPEG TS
DATA LINK LAYER
PHYSICAL LAYER
TRANSPORT PROTOCOL

FIG.6


133 MEDIA SAM
132 RAM REGION
131 ROM REGION
130 ROM TYPE STORAGE MEDIUM

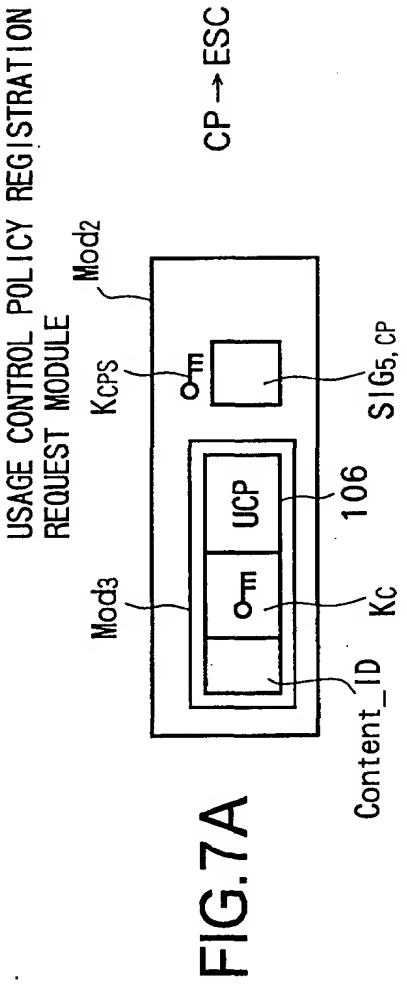

USAGE CONTROL POLICY REGISTRATION REQUEST MODULE
CP→ESC
Mod2
KCPS
SIG5, CP
Mod3
UCP
106
KC
Content_ID

FIG.7A

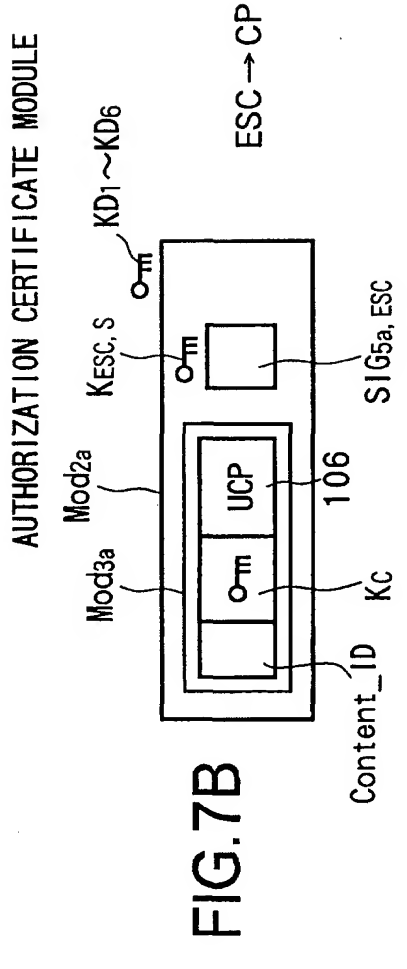
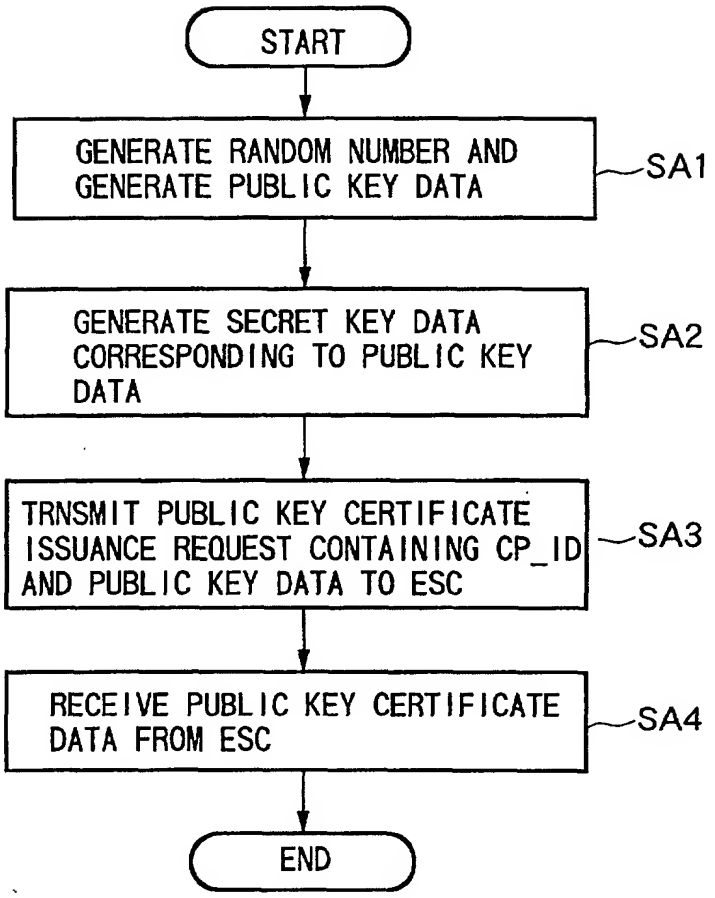

AUTHORIZATION CERTIFICATE MODULE
ESC→CP
KD1~KD6
Mod2a
KESC, S
SIG5a, ESC
Mod3a
UCP
106
KC
Content_ID

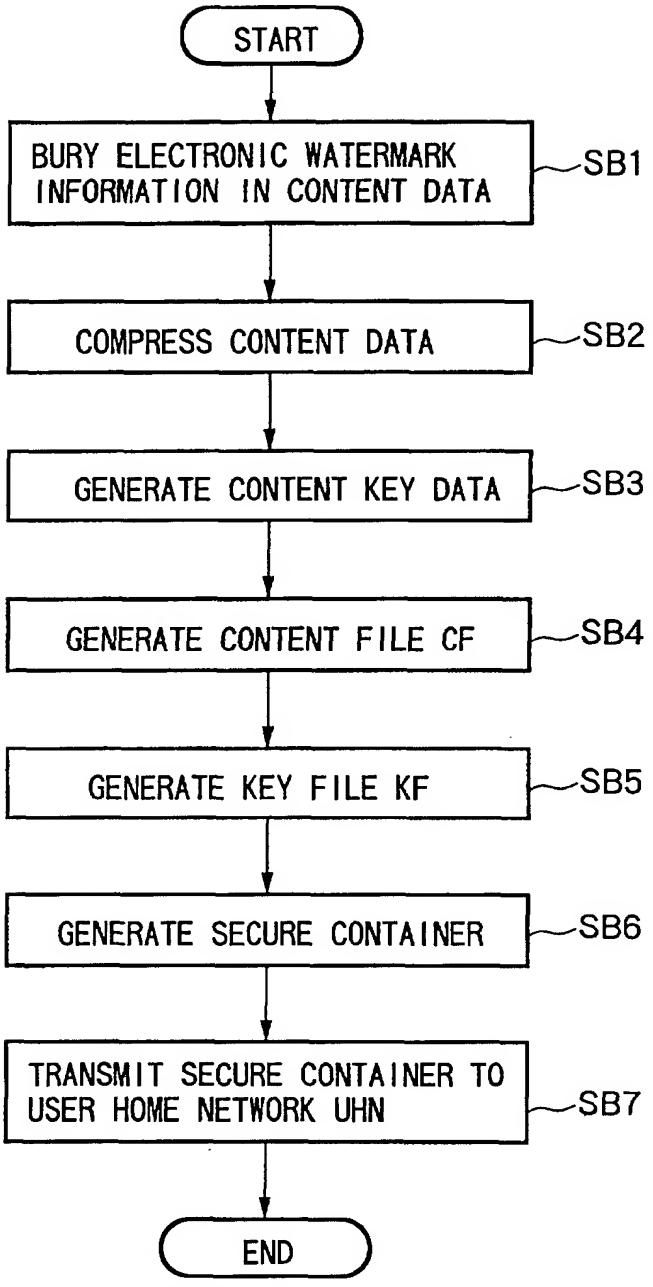
FIG.7B

FIG.8



PROCESSING FOR REQUESTING ISSUANCE OF PUBLIC KEY CERTIFICATE DATA FROM CP TO ESC

FIG.9



PROCESSING FOR PREPARING SECURE CONTAINER OF CP

FIG.10

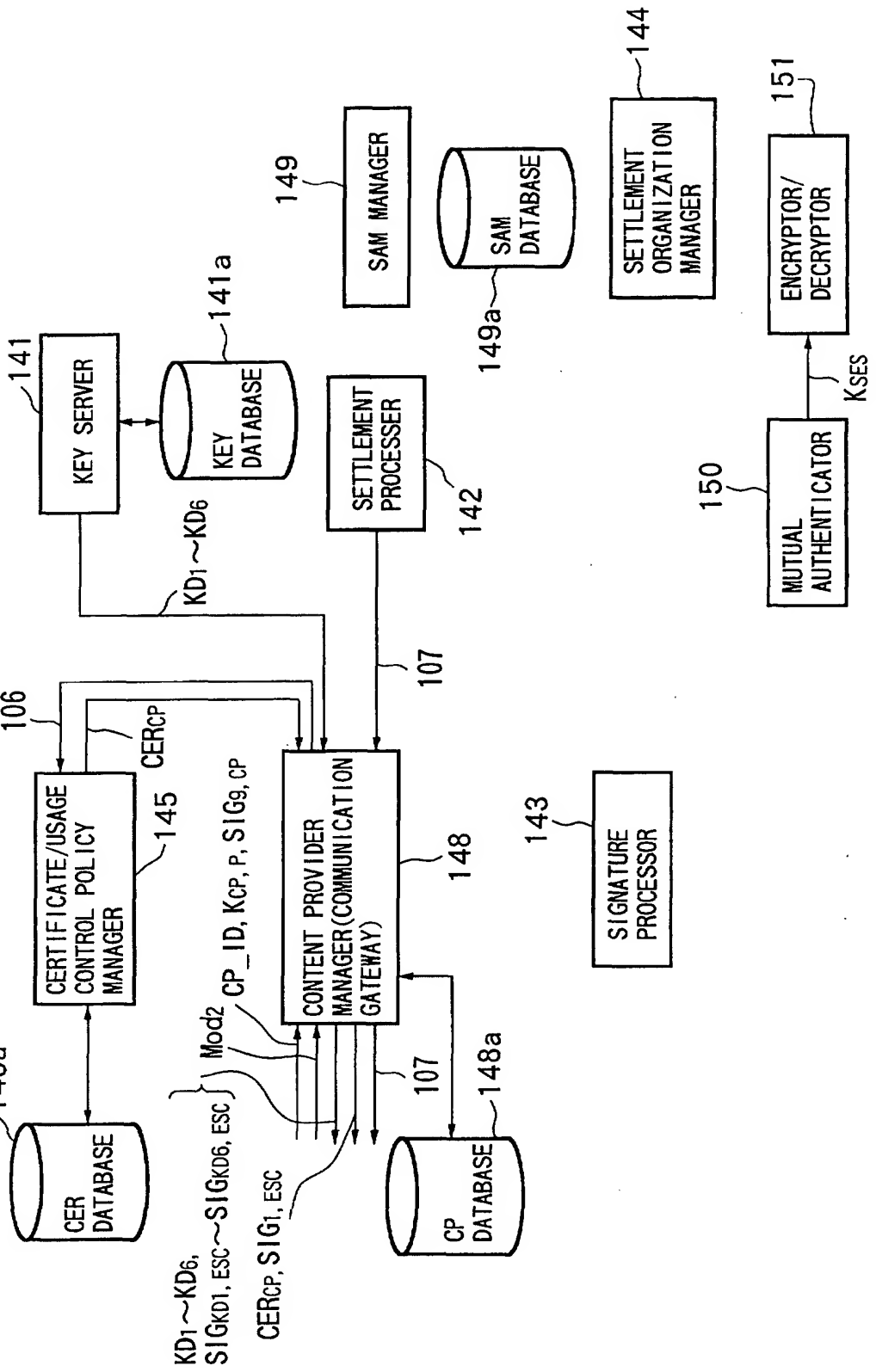

102 EMD SERVICE CENTER
KEY SERVER
141
KEY DATABASE
141a
SAM MANAGER
149
SAM DATABASE
149a
SETTLEMENT ORGANIZATION MANAGER
144
ENCRYPTOR/ DECRYPTOR
151
SETTLEMENT PROCESSER
142
MUTUAL AUTHENTICATOR
150
KSES
KD1~KD6
106
CERCP
107
CERTIFICATE/USAGE CONTROL POLICY MANAGER
145
CONTENT PROVIDER MANAGER(COMMUNICATION GATEWAY)
148
SIGNATURE PROCESSOR
143
CER DATABASE
145a
CP DATABASE
148a
Mod2
CP_ID, KCP, P, SIG9, CP
KD1~KD6, SIGKD1, ESC~SIGKD6, ESC
CERCP, SIG1, ESC

FIG.11

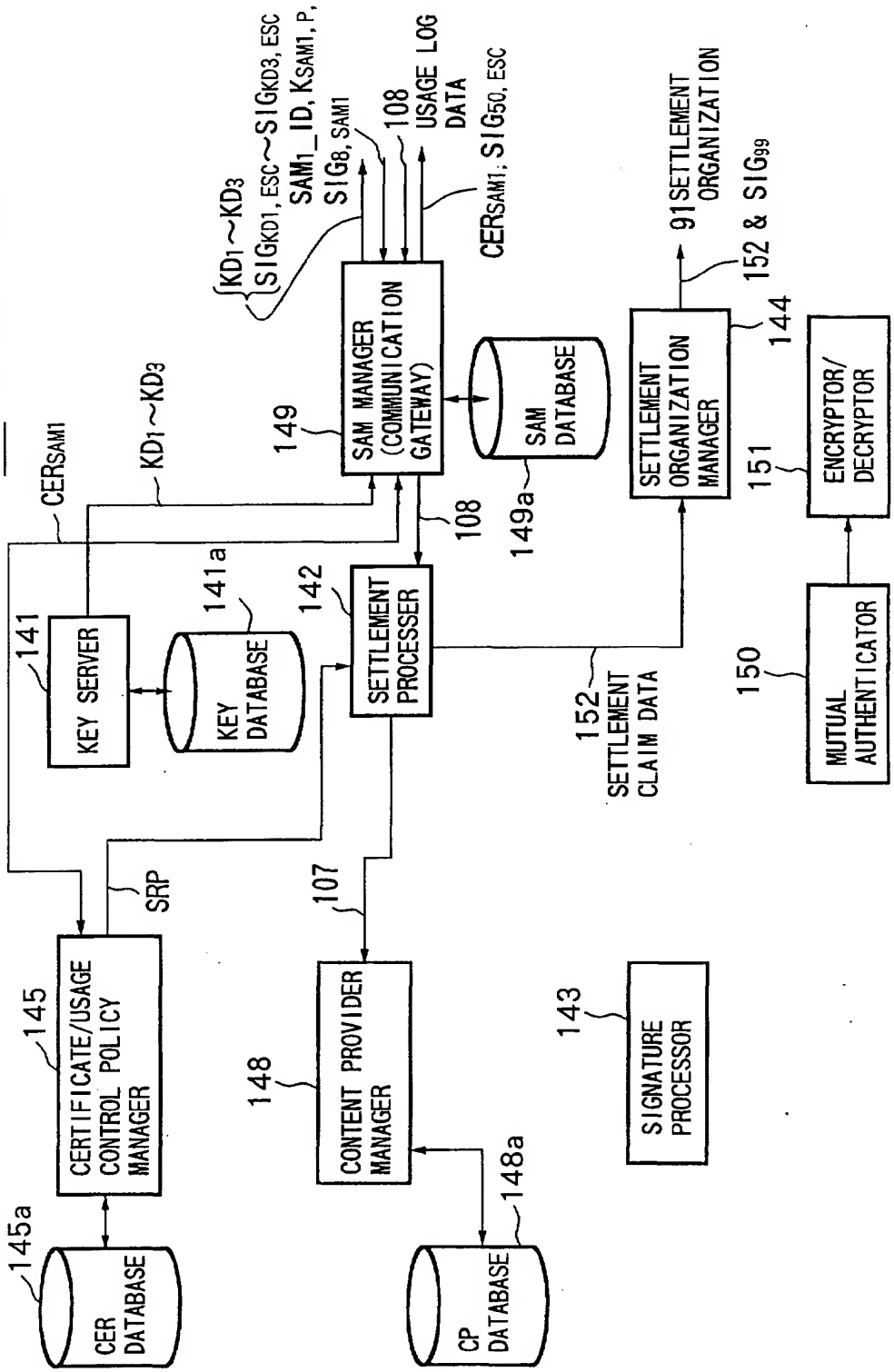
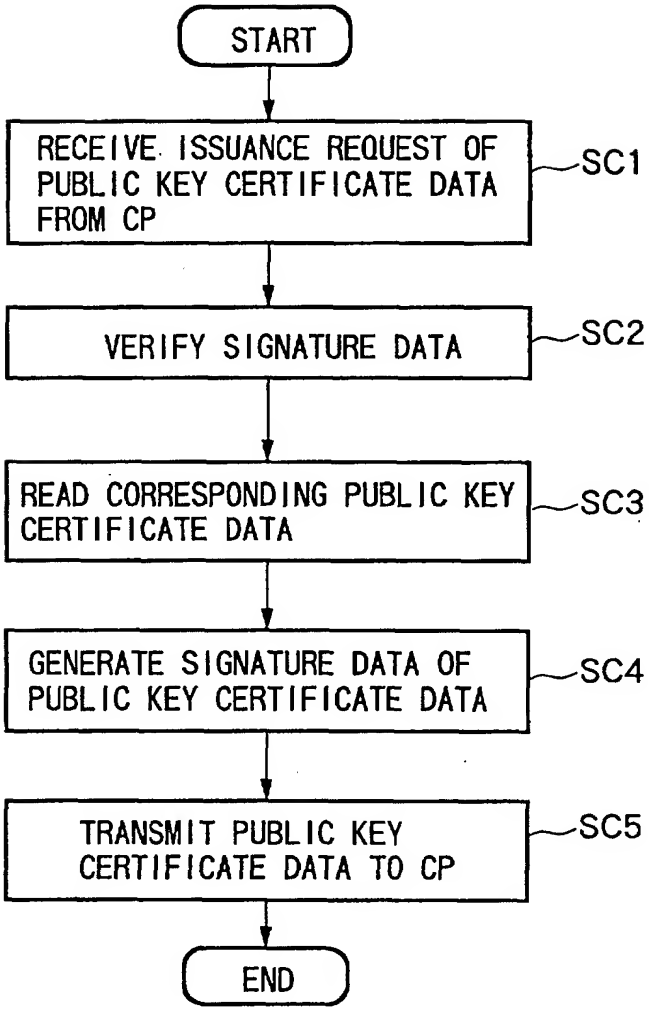
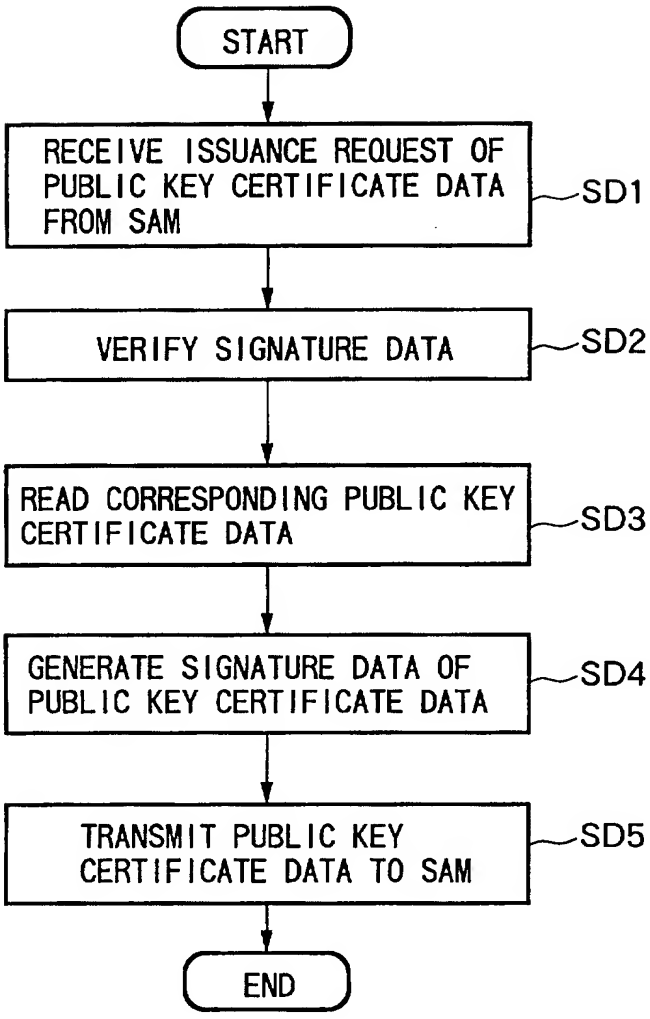

102 EMD SERVICE CENTER
CERSAM1
KD1~KD3
KD1~KD3
SIGKD1, ESC~SIGKD3, ESC
SAM1_ID, KSAM1, P,
SIG8, SAM1
108
USAGE LOG DATA
CERSAM1, SIG50, ESC
91 SETTLEMENT ORGANIZATION
152 & SIG99
149
SAM MANAGER (COMMUNICATION GATEWAY)
SAM DATABASE
149a
108
144
SETTLEMENT ORGANIZATION MANAGER
151
ENCRYPTOR/ DECRYPTOR
141
KEY SERVER
141a
KEY DATABASE
142
SETTLEMENT PROCESSER
152
SETTLEMENT CLAIM DATA
150
MUTUAL AUTHENTICATOR
SRP
107
145
CERTIFICATE/USAGE CONTROL POLICY MANAGER
148
CONTENT PROVIDER MANAGER
143
SIGNATURE PROCESSOR
145a
CER DATABASE
148a
CP DATABASE

FIG.12



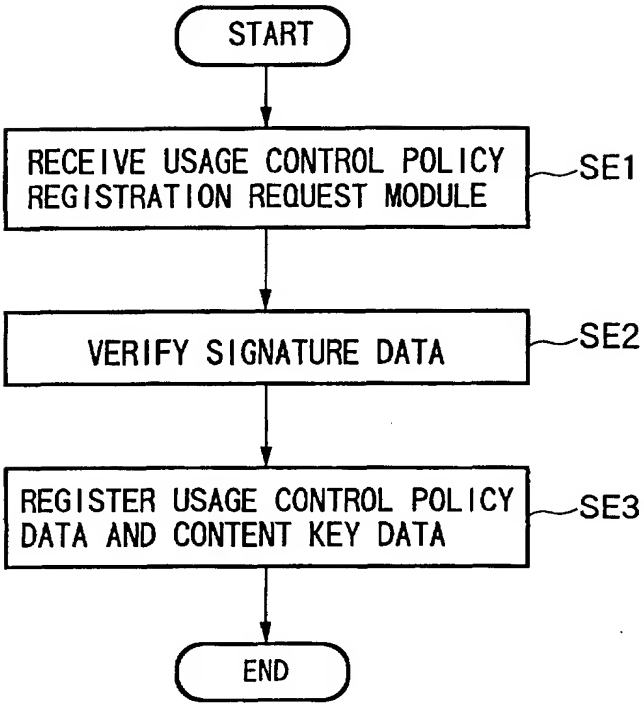
PROCESSING OF ESC IN RESPONSE TO ISSUANCE REQUEST OF PUBLIC KEY CERTIFICATE DATA FROM CP

FIG.13



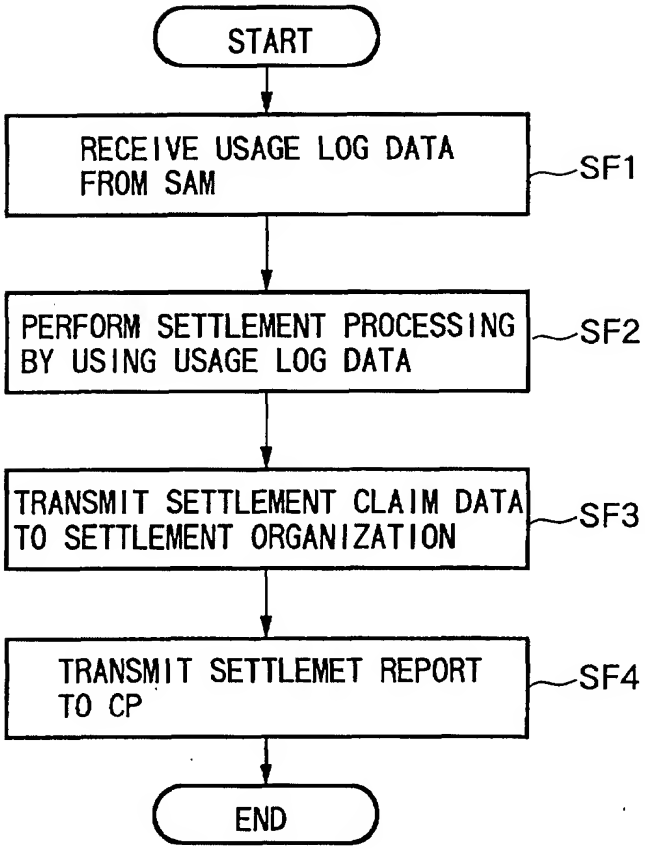
PROCESSING OF ESC IN RESPONSE TO ISSUANCE REQUEST OF PUBLIC KEY CERTIFICATE DATA FROM SAM

FIG.14



PROCESSING FOR REGISTRATION OF USAGE CONTROL POLICY DATA AND CONTENT KEY DATA IN ESC

FIG.15



PROCESSING FOR SETTLEMENT IN ESC

FIG.16

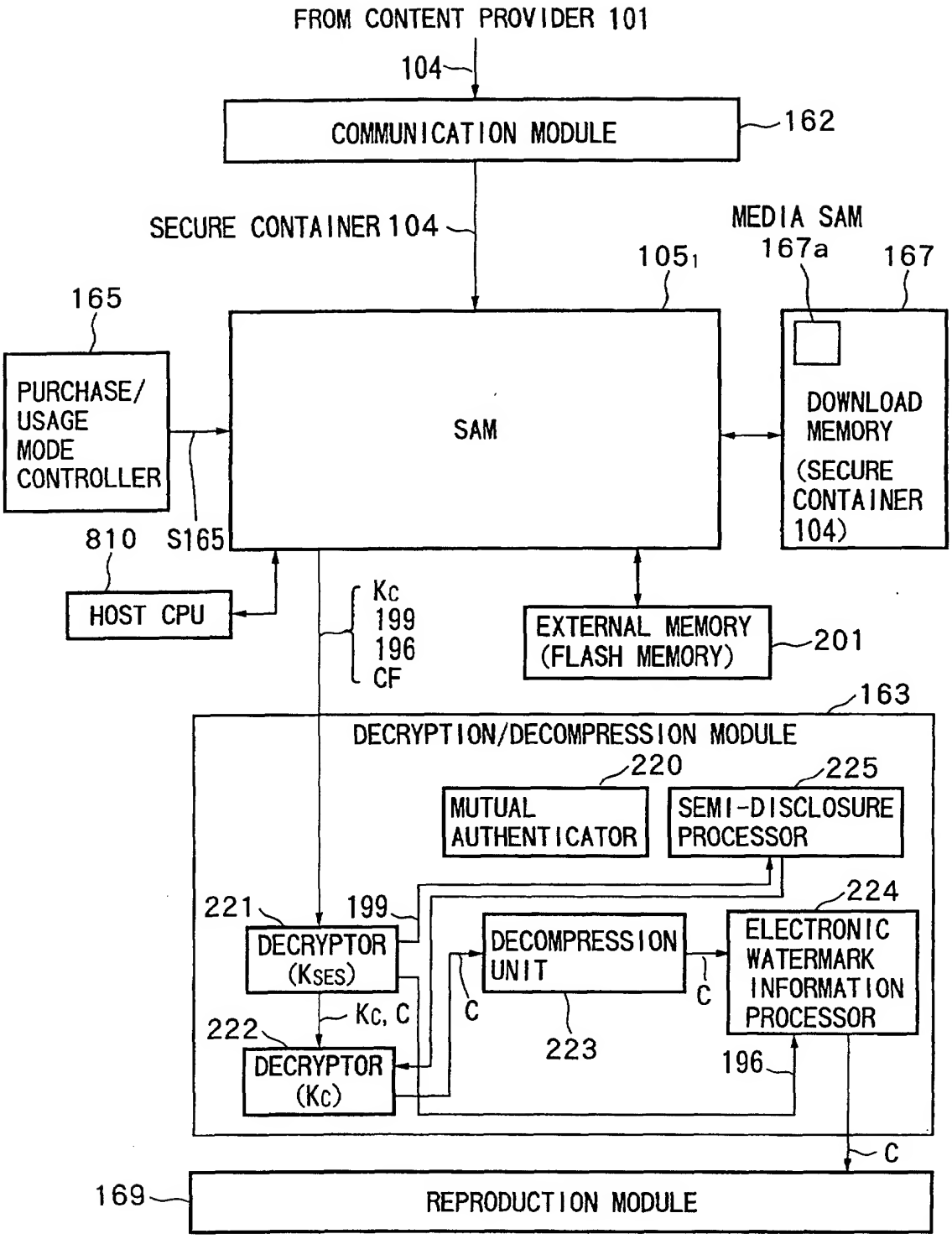

FROM CONTENT PROVIDER 101
104
COMMUNICATION MODULE
162
SECURE CONTAINER 104
MEDIA SAM
167a
167
105₁
165
PURCHASE/ USAGE MODE CONTROLLER
SAM
DOWNLOAD MEMORY (SECURE CONTAINER 104)
810
S165
HOST CPU
Kc
199
196
CF
EXTERNAL MEMORY (FLASH MEMORY)
201
163
DECRYPTION/DECOMPRESSION MODULE
220
225
MUTUAL AUTHENTICATOR
SEMI-DISCLOSURE PROCESSOR
221
199
224
DECRYPTOR (KSES)
DECOMPRESSION UNIT
ELECTRONIC WATERMARK INFORMATION PROCESSOR
Kc, C
C
C
222
223
DECRYPTOR (Kc)
196
C
169
REPRODUCTION MODULE

FIG.17

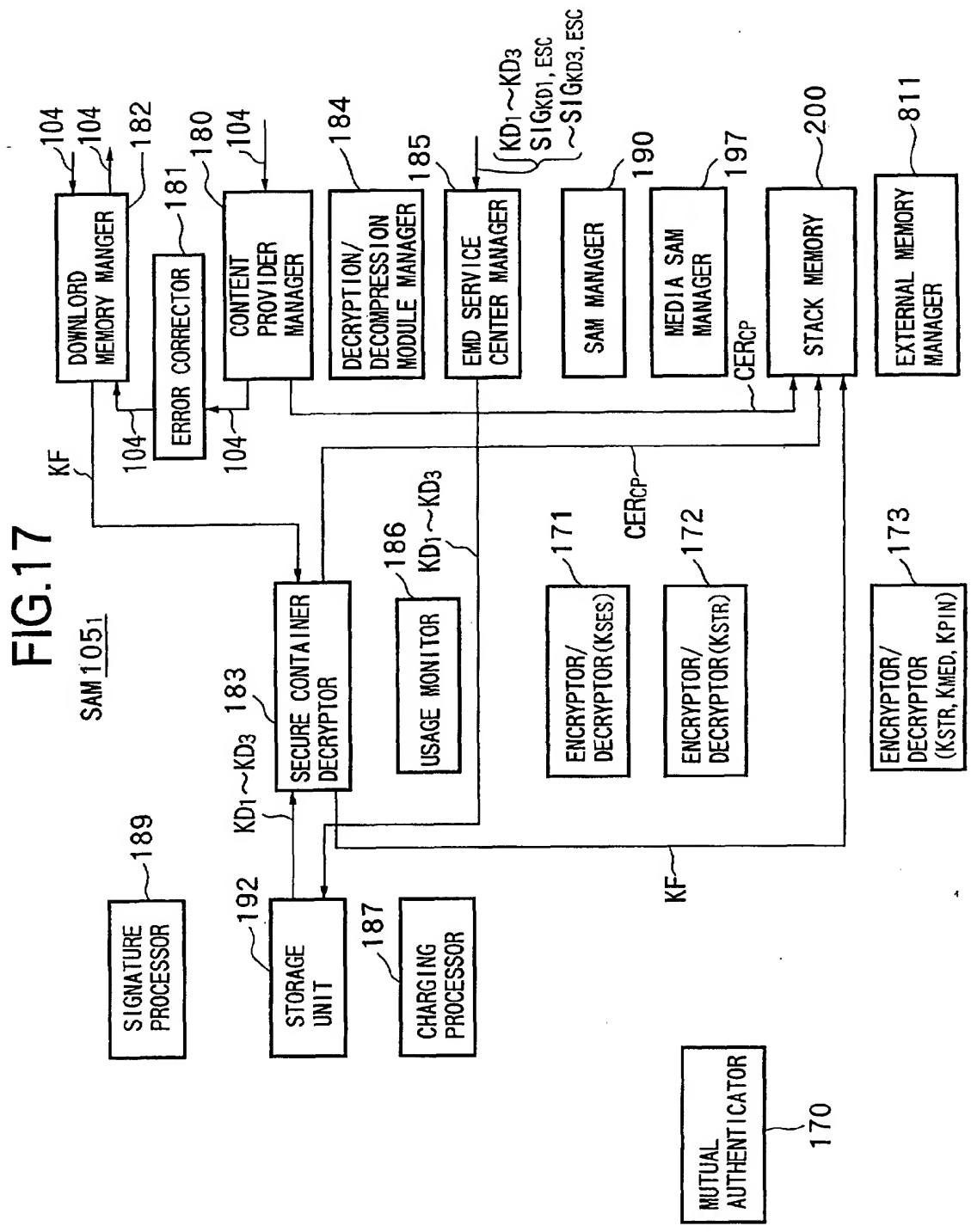

SAM 105₁
DOWNLORD MEMORY MANGER
ERROR CORRECTOR
CONTENT PROVIDER MANAGER
DECRYPTION/ DECOMPRESSION MODULE MANAGER
EMD SERVICE CENTER MANAGER
SAM MANAGER
MEDIA SAM MANAGER
STACK MEMORY
EXTERNAL MEMORY MANAGER
SECURE CONTAINER DECRYPTOR
USAGE MONITOR
ENCRYPTOR/ DECRYPTOR(KSES)
ENCRYPTOR/ DECRYPTOR(KSTR)
ENCRYPTOR/ DECRYPTOR (KSTR, KMED, KPIN)
SIGNATURE PROCESSOR
STORAGE UNIT
CHARGING PROCESSOR
MUTUAL AUTHENTICATOR
KF
CERCP
KD1~KD3
SIGKD1, ESC
SIGKD3, ESC
104
182
181
180
184
185
190
197
200
811
183
186
171
172
173
189
192
187
170

FIG.18

DATA STORED IN EXTERNAL MEMORY 201

USAGE LOG DATA 108
SAM REGISTRATION LIST

FIG.19

DATA STORED IN STACK MEMORY 200

CONTENT KEY DATA Kc
USAGE CONTROL POLICY DATA(USP) 106
LOCK KEY DATA K_{LOG} OF STORAGE UNIT(FLASH MEMORY) 192
PUBLIC KEY CERTIFICATE CER_{CP} OF CONTENT PROVIDER 101
USAGE CONTROL STATUS DATA(UCS) 166
SAM PROGRAM DOWNLORD CONTAINER SD_1 TO SDC_3

FIG.20

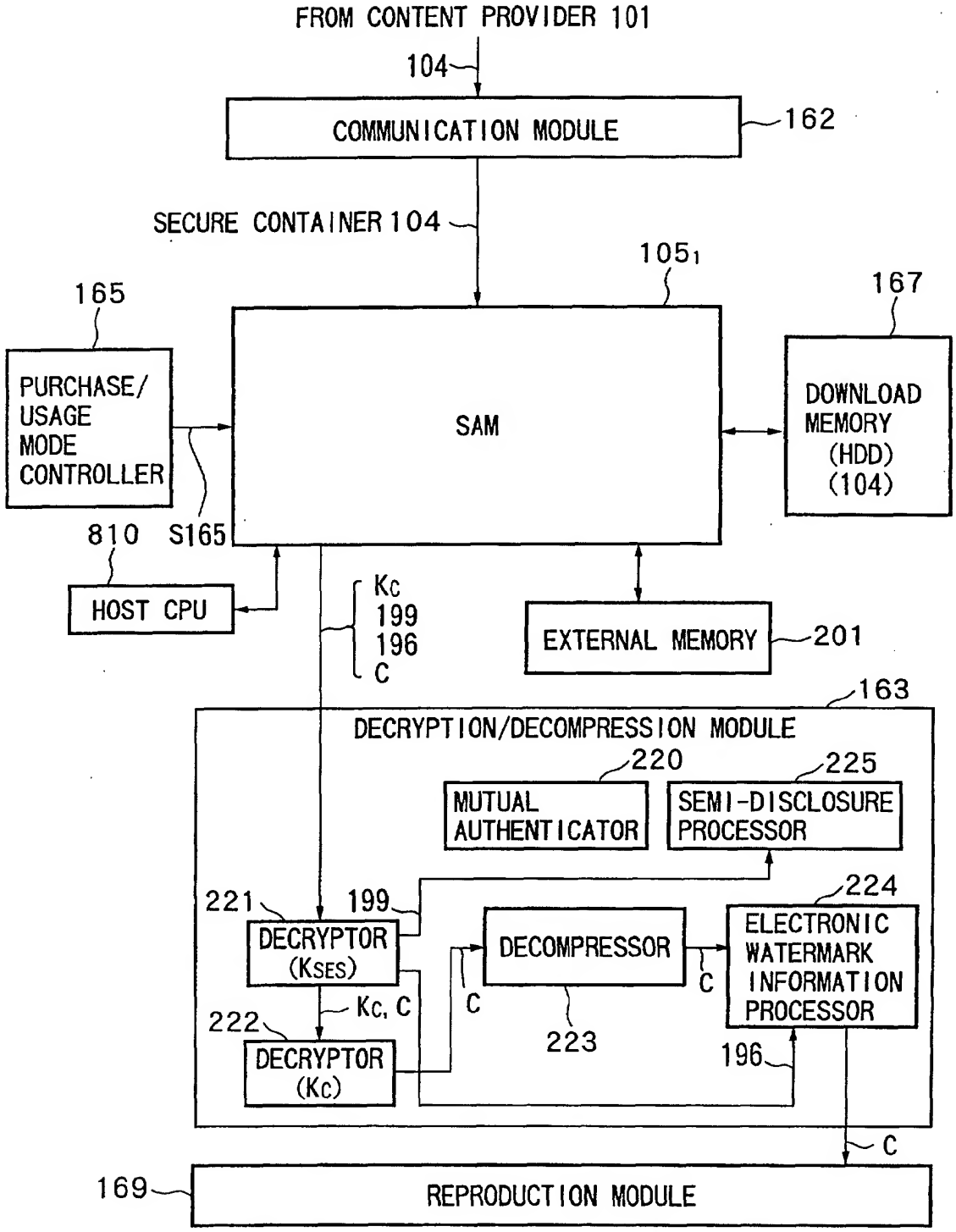

FROM CONTENT PROVIDER 101
104
COMMUNICATION MODULE
162
SECURE CONTAINER 104
105_1
165
167
PURCHASE/ USAGE MODE CONTROLLER
SAM
DOWNLOAD MEMORY (HDD) (104)
810
S165
HOST CPU
Kc
199
196
C
EXTERNAL MEMORY
201
163
DECRYPTION/DECOMPRESSION MODULE
220
225
MUTUAL AUTHENTICATOR
SEMI-DISCLOSURE PROCESSOR
221
199
224
DECRYPTOR (KSES)
DECOMPRESSOR
ELECTRONIC WATERMARK INFORMATION PROCESSOR
C
Kc, C
C
222
223
196
DECRYPTOR (Kc)
C
169
REPRODUCTION MODULE

FIG.21

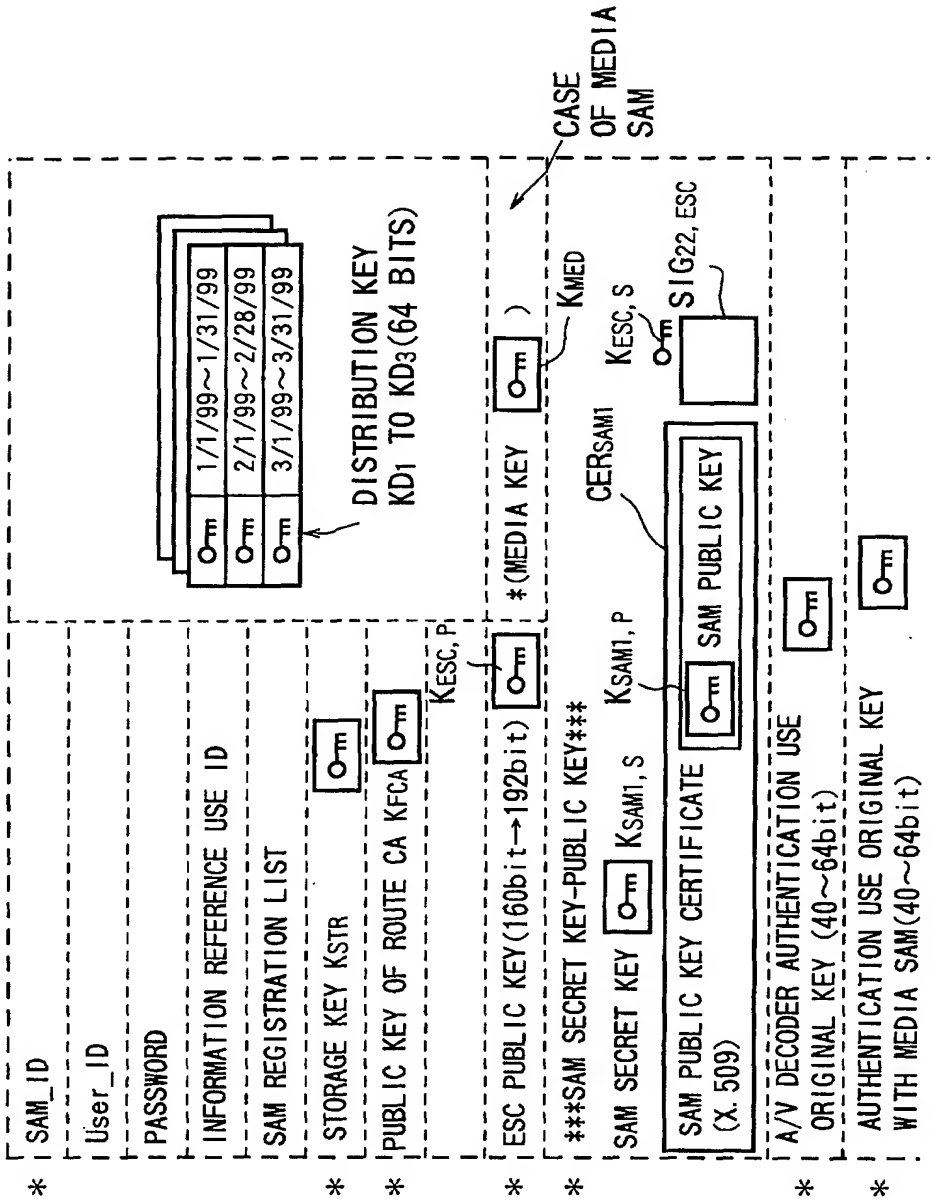
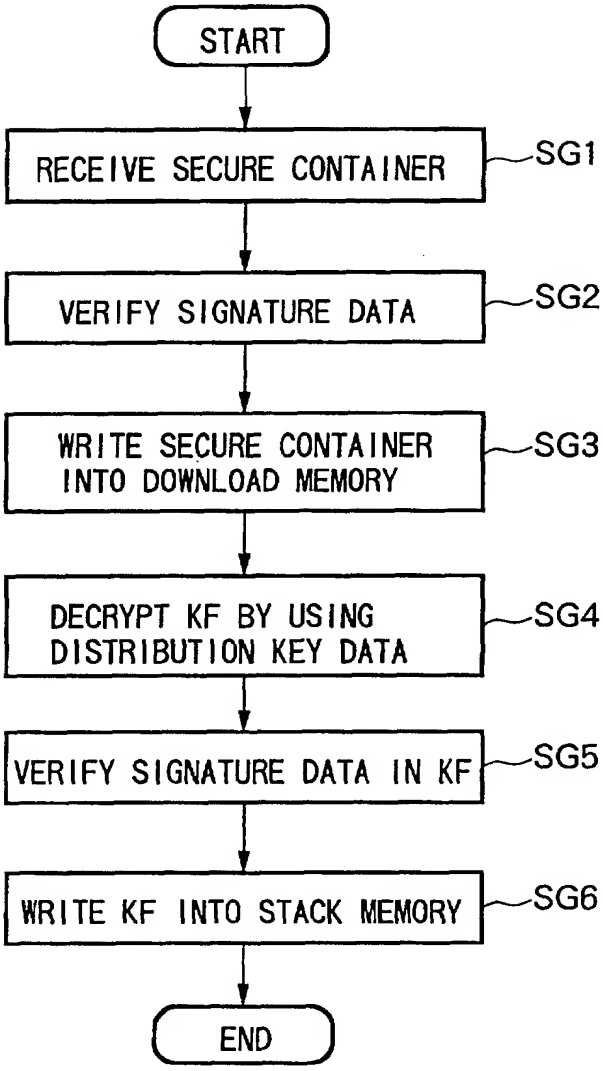

DATA STORED IN STORAGE UNIT 192
SAM_ID
User_ID
PASSWORD
INFORMATION REFERENCE USE ID
SAM REGISTRATION LIST
STORAGE KEY KSTR
PUBLIC KEY OF ROUTE CA KFCA
KESC, P
ESC PUBLIC KEY(160bit→192bit)
SAM SECRET KEY-PUBLIC KEY
SAM SECRET KEY KSAM1, S
SAM PUBLIC KEY CERTIFICATE (X.509)
A/V DECODER AUTHENTICATION USE ORIGINAL KEY (40~64bit)
AUTHENTICATION USE ORIGINAL KEY WITH MEDIA SAM(40~64bit)
1/1/99~1/31/99
2/1/99~2/28/99
3/1/99~3/31/99
DISTRIBUTION KEY
KD1 TO KD3(64 BITS)
*(MEDIA KEY)
KMED
CASE OF MEDIA SAM
CERSAM1
KSAM1, P
SAM PUBLIC KEY
KESC, S
SIG22, ESC

FIG.22



PROCESSING FOR DECRYPTION OF KF IN SAM

FIG.23

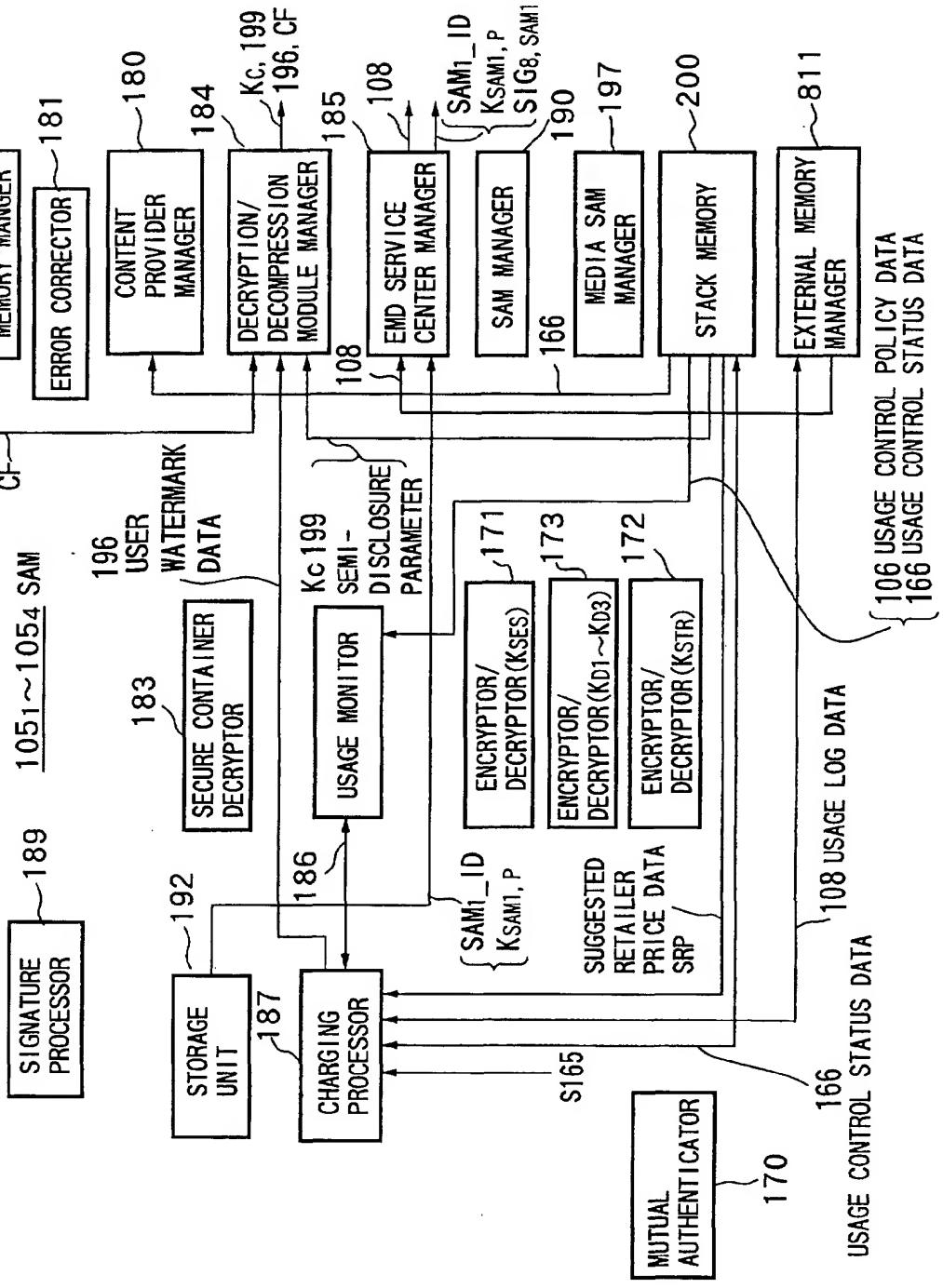
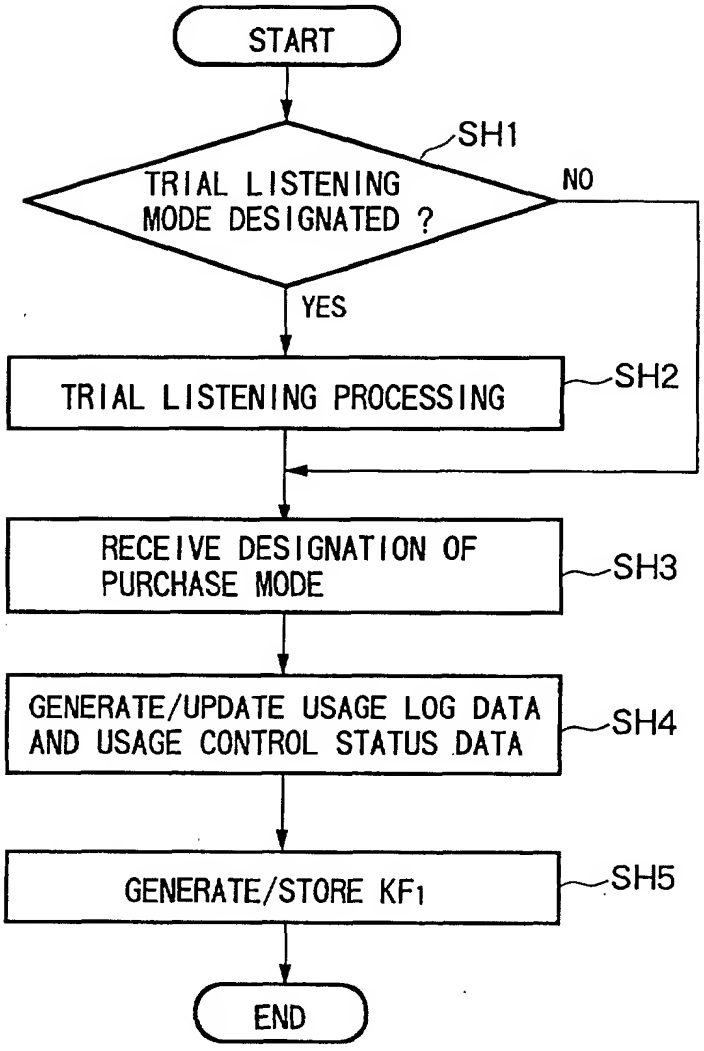
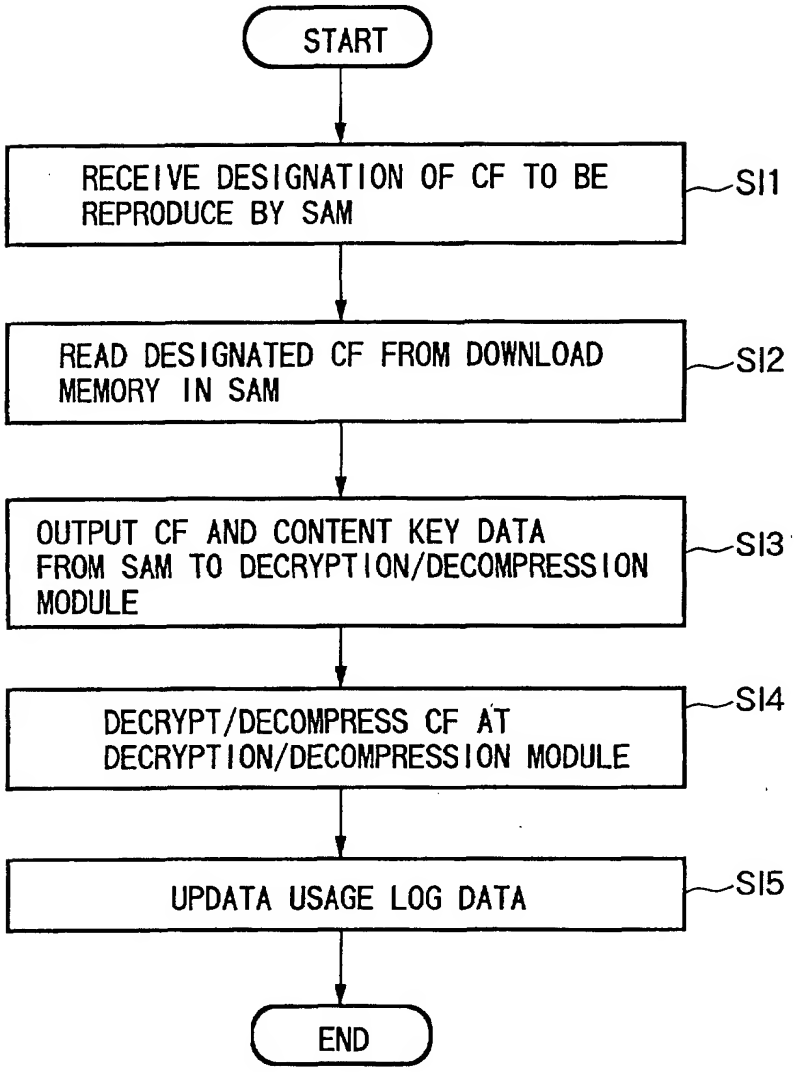

DOWNLORD MEMORY MANGER
182
ERROR CORRECTOR
181
CONTENT PROVIDER MANAGER
180
DECRYPTION/ DECOMPRESSION MODULE MANAGER
184
Kc, 199
196, CF
185
EMD SERVICE CENTER MANAGER
108
SAM1_ID
KSAM1, P
SIG8, SAM1
SAM MANAGER
190
MEDIA SAM MANAGER
197
STACK MEMORY
200
EXTERNAL MEMORY MANAGER
811
CF
108
166
196 USER WATERMARK DATA
Kc 199 SEMI-DISCLOSURE PARAMETER
105₁~105₄ SAM
183
SECURE CONTAINER DECRYPTOR
USAGE MONITOR
186
171
ENCRYPTOR/ DECRYPTOR(KSES)
173
ENCRYPTOR/ DECRYPTOR(KD1~KD3)
172
ENCRYPTOR/ DECRYPTOR(KSTR)
106 USAGE CONTROL POLICY DATA
166 USAGE CONTROL STATUS DATA
189
SIGNATURE PROCESSOR
192
STORAGE UNIT
187
CHARGING PROCESSOR
SAMi_ID
KSAM1, P
SUGGESTED RETAILER PRICE DATA SRP
108 USAGE LOG DATA
S165
166
USAGE CONTROL STATUS DATA
MUTUAL AUTHENTICATOR
170

FIG.24



PROCESSING FOR DETERMINATION OF PURCHASE MODE OF SECURE CONTAINER IN SAM

FIG.25



PROCESSING FOR REPRODUCTION OF CONTENT DATA

FIG.26

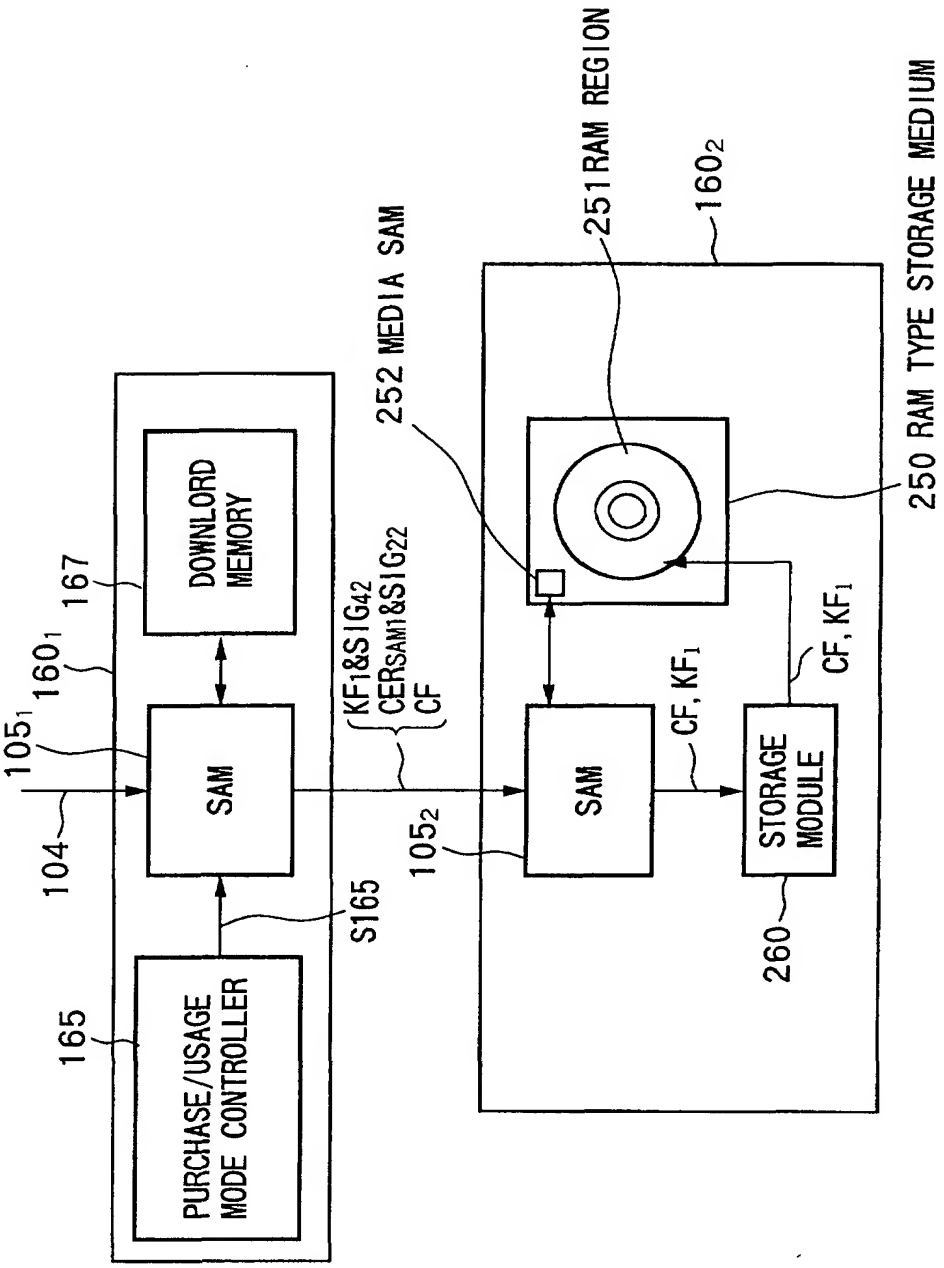

250 RAM TYPE STORAGE MEDIUM
251 RAM REGION
252 MEDIA SAM
160_2
160_1
167
DOWNLORD MEMORY
105_1
SAM
104
165
PURCHASE/USAGE MODE CONTROLLER
S165
KF_1&SIG_{42}
CER_{SAM1}&SIG_{22}
CF
105_2
SAM
CF, KF_1
STORAGE MODULE
260
CF, KF_1

FIG27

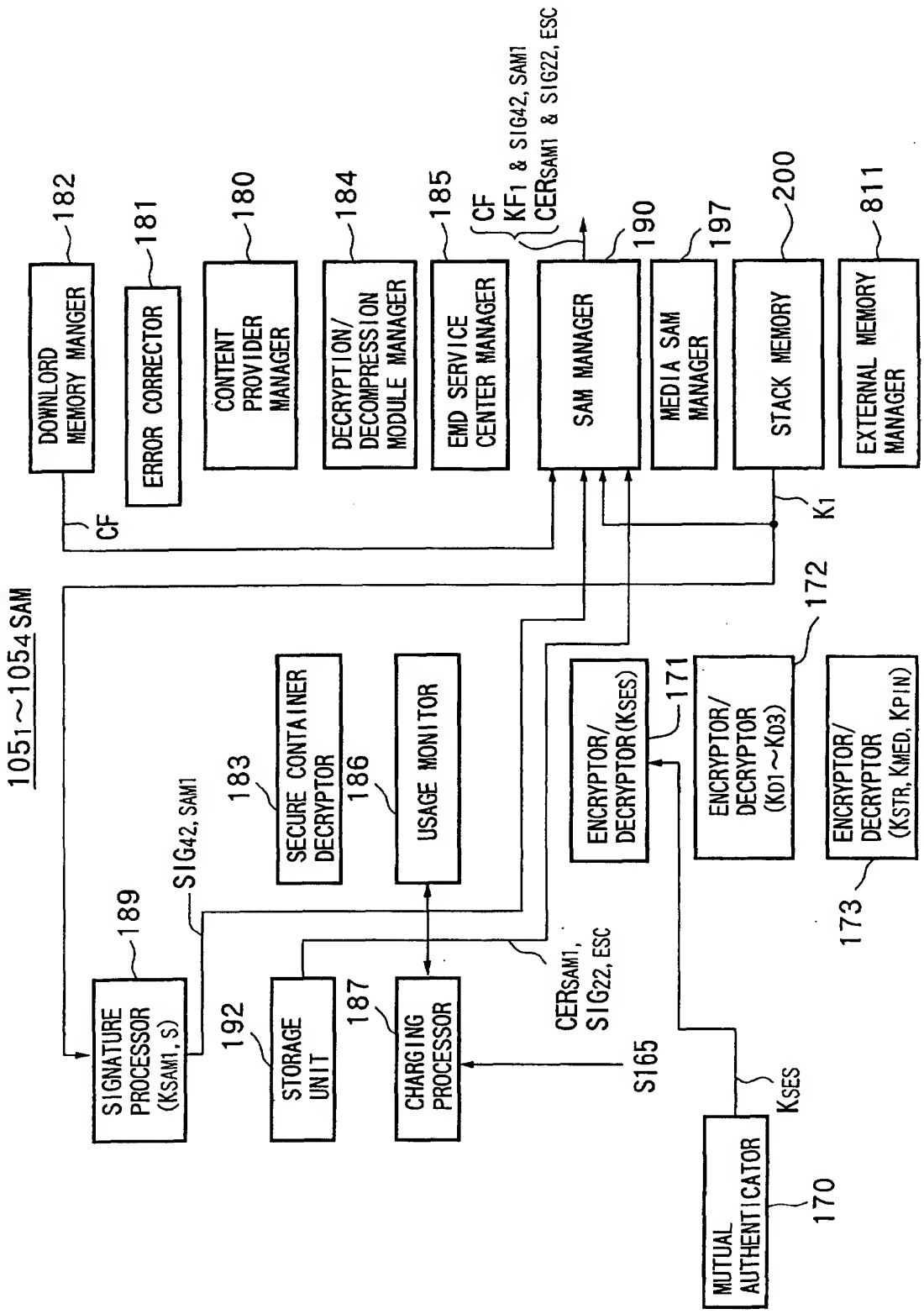
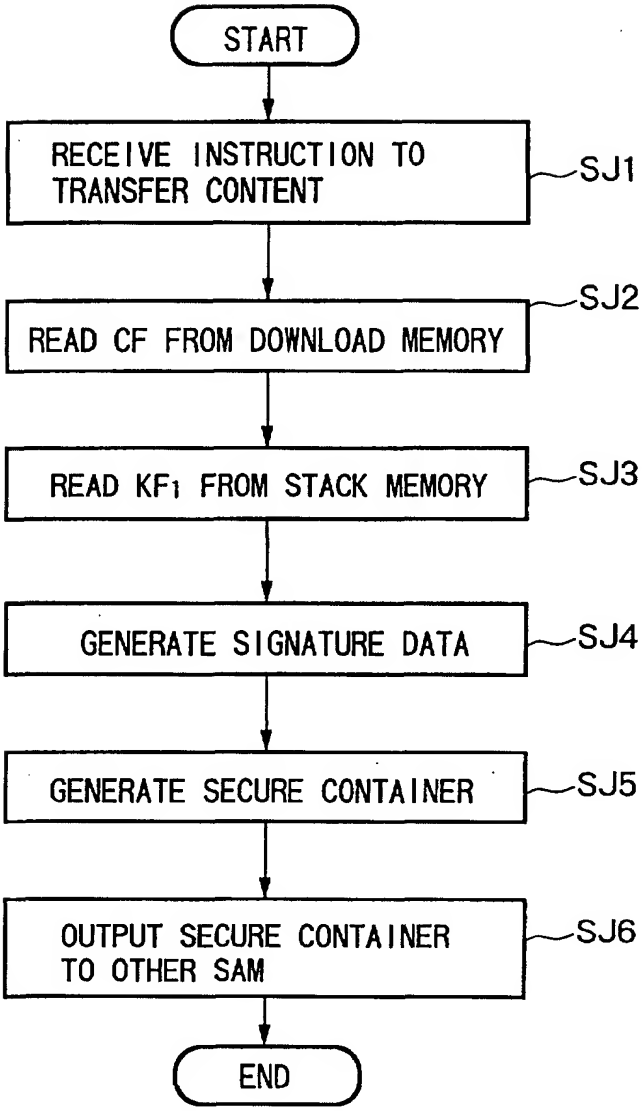

105₁~105₄ SAM
DOWNLORD MEMORY MANGER
182
ERROR CORRECTOR
181
CONTENT PROVIDER MANAGER
180
DECRYPTION/ DECOMPRESSION MODULE MANAGER
184
EMD SERVICE CENTER MANAGER
185
CF
KF1 & SIG42, SAM1
CERSAM1 & SIG22, ESC
SAM MANAGER
190
MEDIA SAM MANAGER
197
STACK MEMORY
200
EXTERNAL MEMORY MANAGER
811
CF
K1
SECURE CONTAINER DECRYPTOR
183
USAGE MONITOR
186
ENCRYPTOR/ DECRYPTOR(KSES)
171
ENCRYPTOR/ DECRYPTOR (KD1~KD3)
172
ENCRYPTOR/ DECRYPTOR (KSTR, KMED, KPIN)
173
SIGNATURE PROCESSOR (KSAM1, S)
189
SIG42, SAM1
STORAGE UNIT
192
CHARGING PROCESSOR
187
CERSAM1, SIG22, ESC
S165
KSES
MUTUAL AUTHENTICATOR
170

FIG.28



PROCESSING OF SAM FOR TRANSFERRING CONTENT AFTER DETERMINING PURCHASE MODE TO OTHER SAM

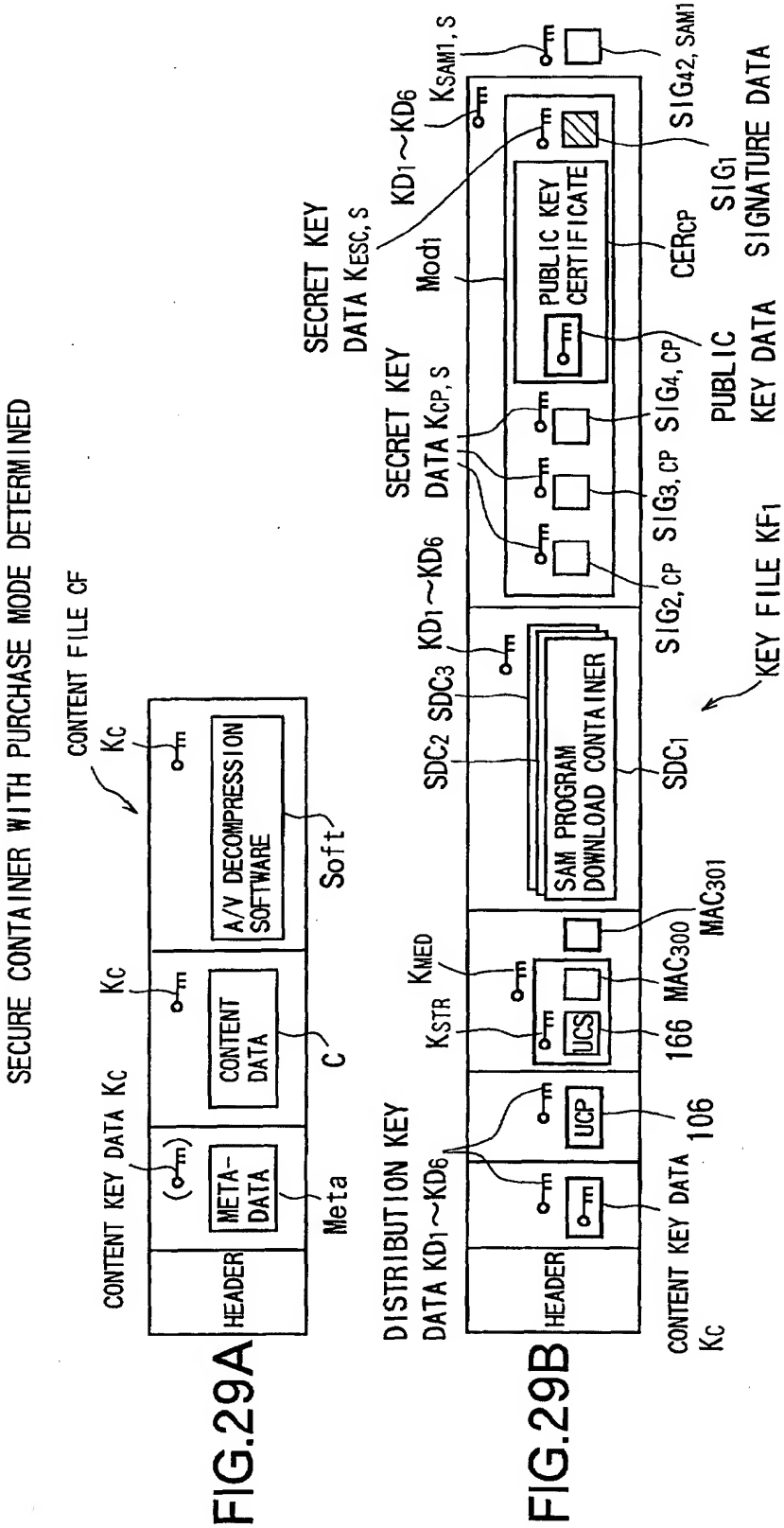

SECURE CONTAINER WITH PURCHASE MODE DETERMINED
CONTENT FILE CF
Kc
CONTENT KEY DATA Kc
HEADER
META-DATA
Meta
CONTENT DATA
C
A/V DECOMPRESSION SOFTWARE
Soft
FIG.29A
DISTRIBUTION KEY DATA KD1~KD6
SDC2 SDC3
KD1~KD6
SECRET KEY DATA KESC, S
SECRET KEY DATA KCP, S
Mod1
KSAM1, S
PUBLIC KEY CERTIFICATE
CERCP
SIG42, SAM1
SIG1
SIGNATURE DATA
PUBLIC KEY DATA KCP, P
KEY FILE KF1
SIG2, CP
SIG3, CP
SIG4, CP
KSTR
KMED
UCP
UCS
166
MAC300
MAC301
SAM PROGRAM DOWNLOAD CONTAINER
SDC1
106
CONTENT KEY DATA Kc
FIG.29B
KESC, S
SIG22, ESC
PUBLIC KEY CERTIFICATE
KSAM1, P
CERSAM1
FIG.29C

FIG.30

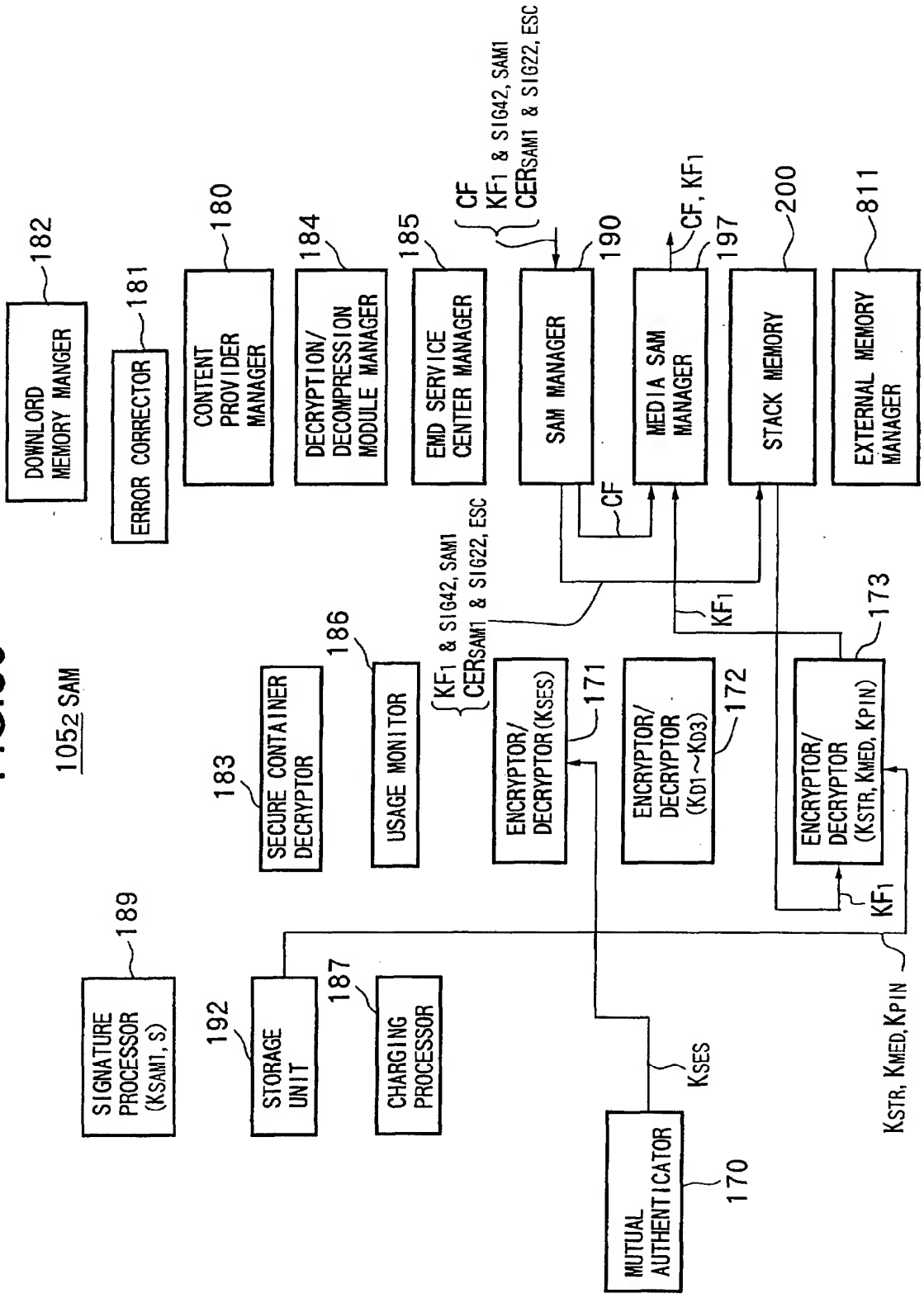
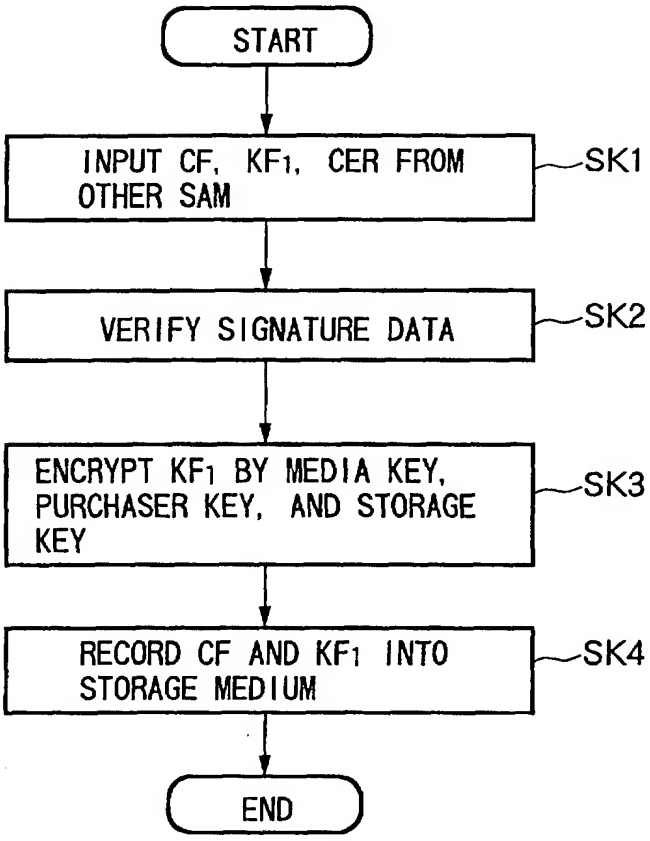

1052 SAM
DOWNLORD MEMORY MANGER
182
ERROR CORRECTOR
181
CONTENT PROVIDER MANAGER
180
DECRYPTION/ DECOMPRESSION MODULE MANAGER
184
EMD SERVICE CENTER MANAGER
185
CF
KF1 & SIG42, SAM1
CERSAM1 & SIG22, ESC
SAM MANAGER
190
MEDIA SAM MANAGER
CF, KF1
197
STACK MEMORY
200
EXTERNAL MEMORY MANAGER
811
CF
KF1 & SIG42, SAM1
CERSAM1 & SIG22, ESC
KF1
173
SECURE CONTAINER DECRYPTOR
183
USAGE MONITOR
186
ENCRYPTOR/ DECRYPTOR (KSES)
171
ENCRYPTOR/ DECRYPTOR (KD1~KD3)
172
ENCRYPTOR/ DECRYPTOR (KSTR, KMED, KPIN)
KF1
SIGNATURE PROCESSOR (KSAM1, S)
189
STORAGE UNIT
192
CHARGING PROCESSOR
187
MUTUAL AUTHENTICATOR
170
KSES
KSTR, KMED, KPIN

FIG.31



PROCESSING OF SAM WHEN WRITING CF, ETC. INPUT FROM OTHER SAM INTO STORAGE MEDIUM

FIG.32

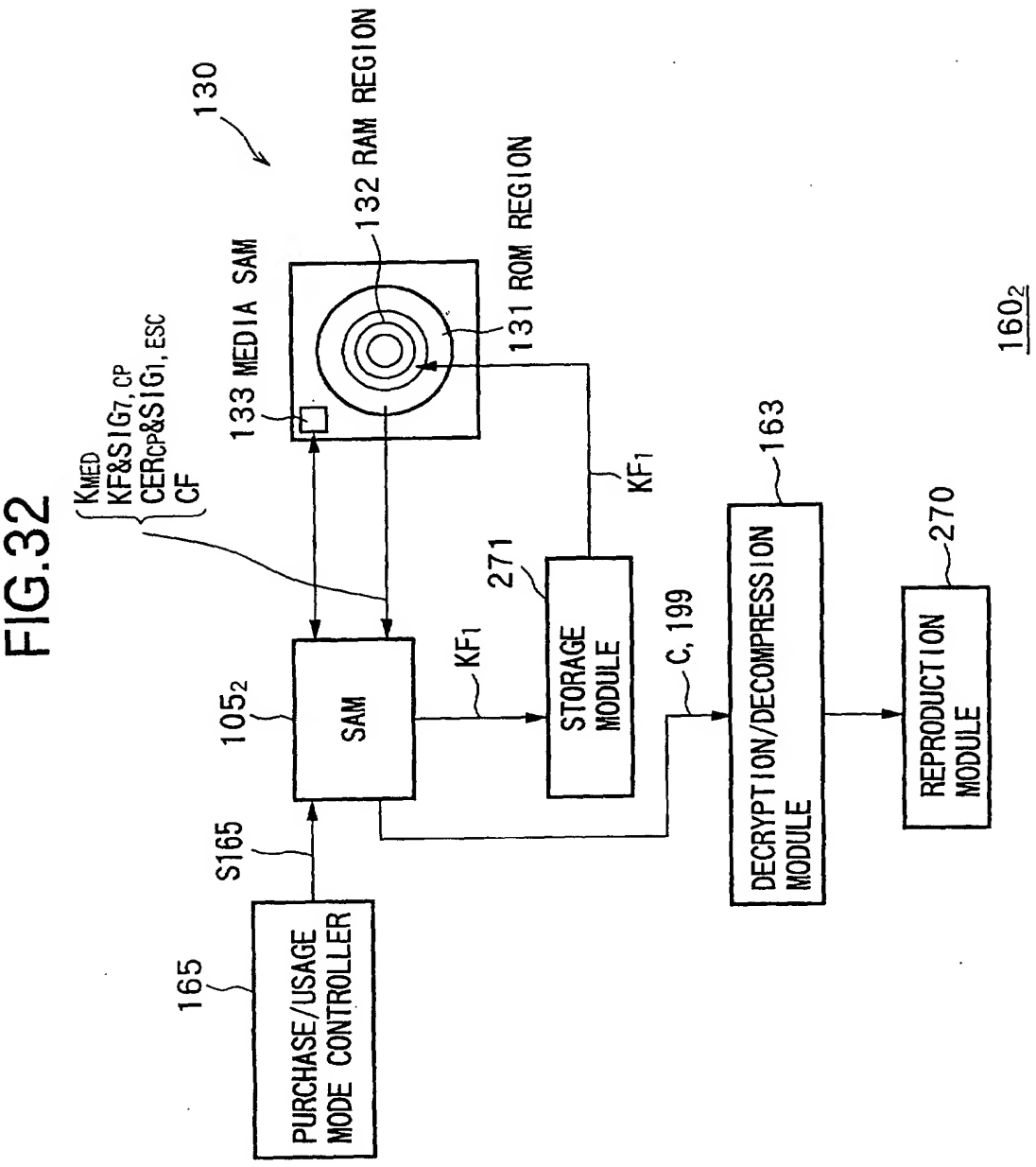

130
132 RAM REGION
131 ROM REGION
133 MEDIA SAM
K_{MED}
$KF\&SIG_{7,CP}$
$CER_{CP}\&SIG_{1,ESC}$
CF
KF_1
271
STORAGE MODULE
KF_1
105_2
SAM
C, 199
163
DECRYPTION/DECOMPRESSION MODULE
270
REPRODUCTION MODULE
S165
165
PURCHASE/USAGE MODE CONTROLLER
160_2

FIG.33

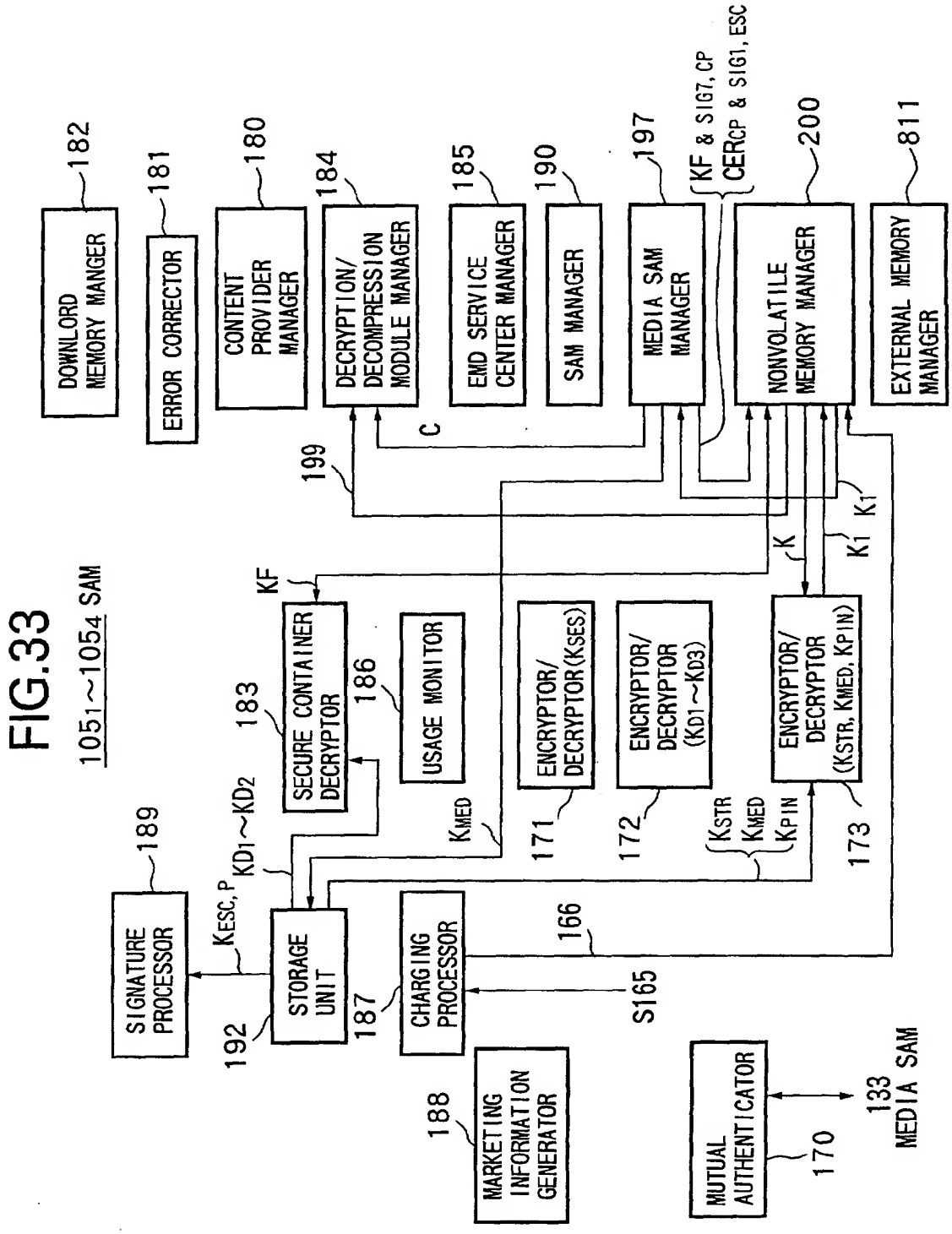
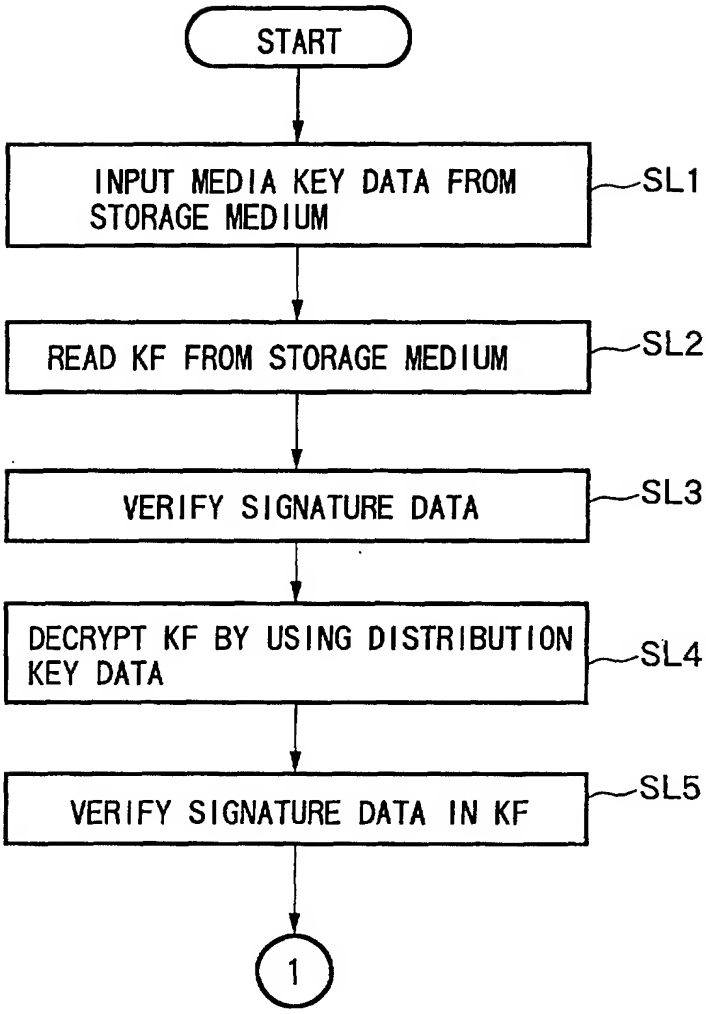
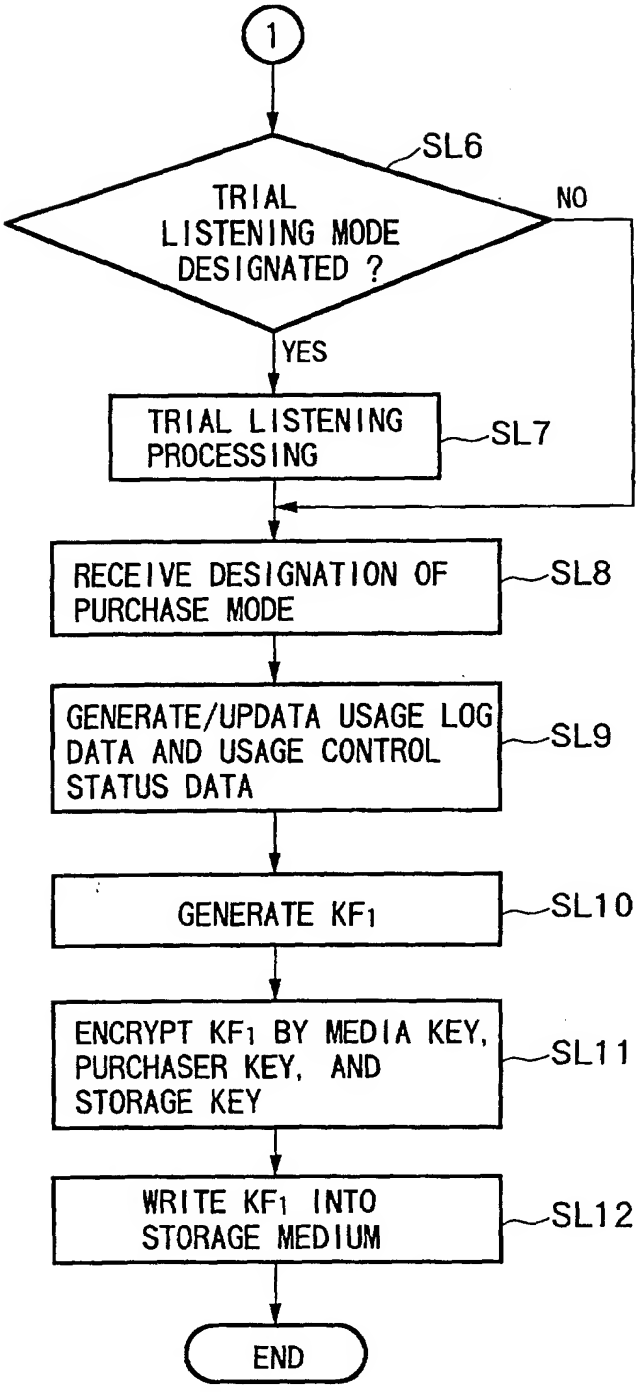

DOWNLORD MEMORY MANGER
182
ERROR CORRECTOR
181
CONTENT PROVIDER MANAGER
180
DECRYPTION/ DECOMPRESSION MODULE MANAGER
184
EMD SERVICE CENTER MANAGER
185
SAM MANAGER
190
MEDIA SAM MANAGER
197
NONVOLATILE MEMORY MANAGER
200
EXTERNAL MEMORY MANAGER
811
KF & SIG7, CP
CERCP & SIG1, ESC
C
199
K
K1
K1
KF
1051~1054 SAM
SECURE CONTAINER DECRYPTOR
183
186
USAGE MONITOR
ENCRYPTOR/ DECRYPTOR(KSES)
171
ENCRYPTOR/ DECRYPTOR (KD1~KD3)
172
ENCRYPTOR/ DECRYPTOR (KSTR, KMED, KPIN)
173
KSTR
KMED
KPIN
KMED
189
SIGNATURE PROCESSOR
KESC, P
KD1~KD2
192
STORAGE UNIT
187
CHARGING PROCESSOR
166
S165
188
MARKETING INFORMATION GENERATOR
MUTUAL AUTHENTICATOR
170
133
MEDIA SAM

FIG.34



PROCESSING FOR DETERMINATION OF PURCHASE MODE IN SAM OF CONTENT DISTRIBUTED ON-LINE

FIG.35



PROCESSING FOR DETEMINATION OF PURCHASE MODE OF CONTENT DISTRIBUTED ON-LINE IN SAM

FIG.36

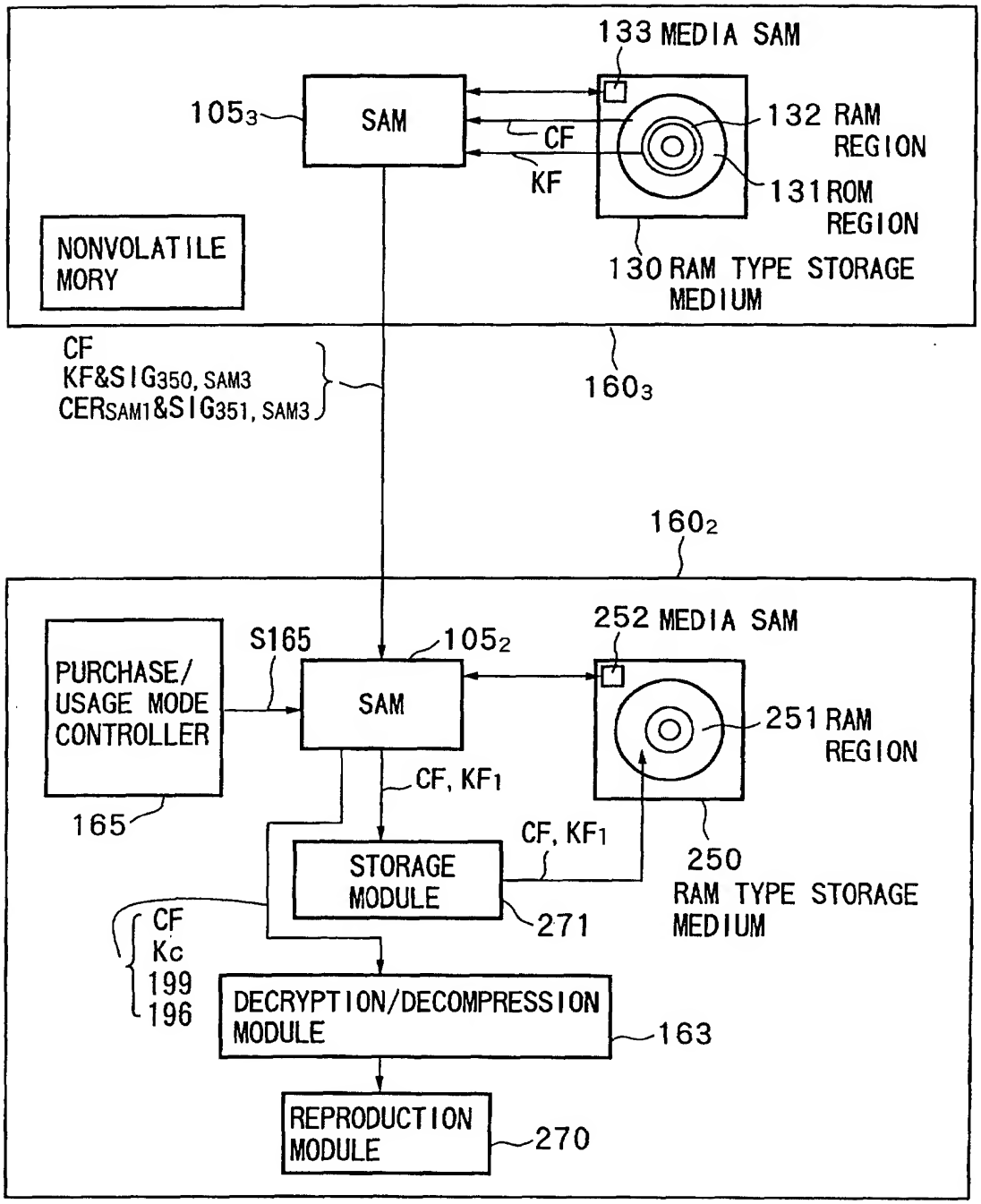
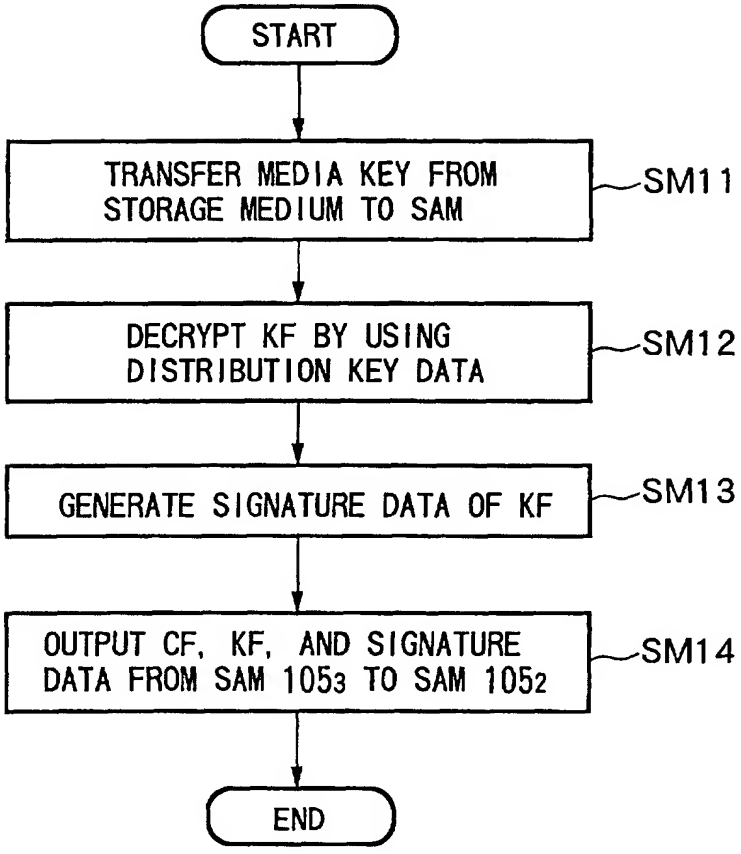
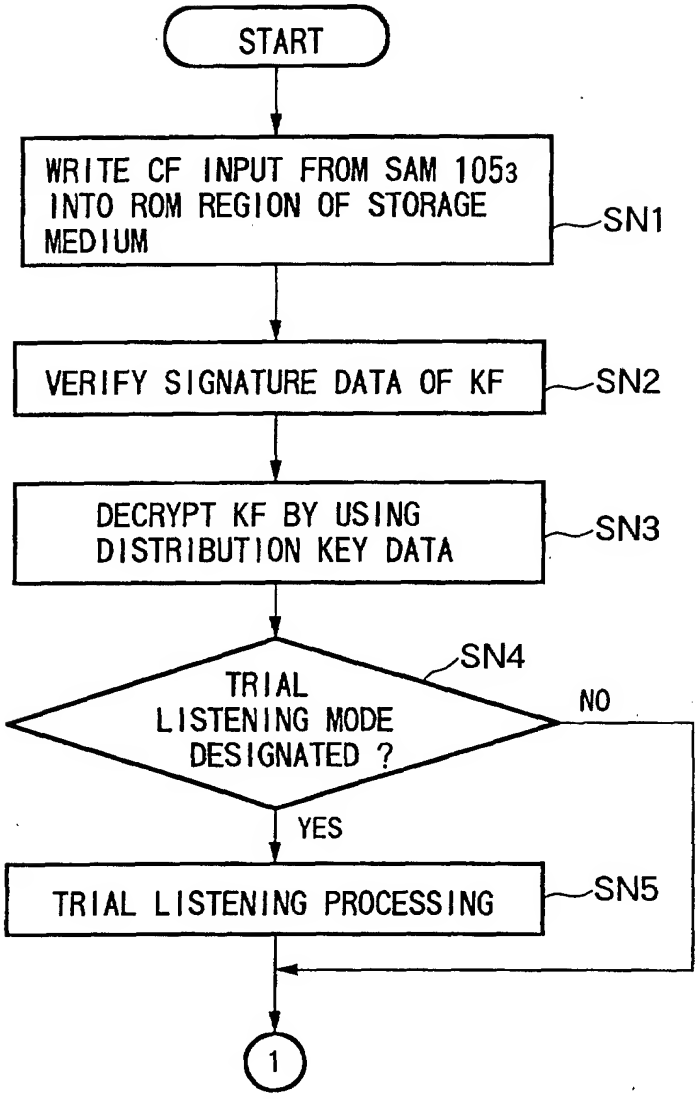

133 MEDIA SAM
105_3
SAM
CF
KF
132 RAM REGION
131 ROM REGION
NONVOLATILE MORY
130 RAM TYPE STORAGE MEDIUM
CF
KF&SIG350, SAM3
CERSAM1&SIG351, SAM3
160_3
160_2
PURCHASE/ USAGE MODE CONTROLLER
S165
105_2
SAM
252 MEDIA SAM
251 RAM REGION
CF, KF1
165
CF, KF1
STORAGE MODULE
271
250 RAM TYPE STORAGE MEDIUM
CF
Kc
199
196
DECRYPTION/DECOMPRESSION MODULE
163
REPRODUCTION MODULE
270

FIG.37



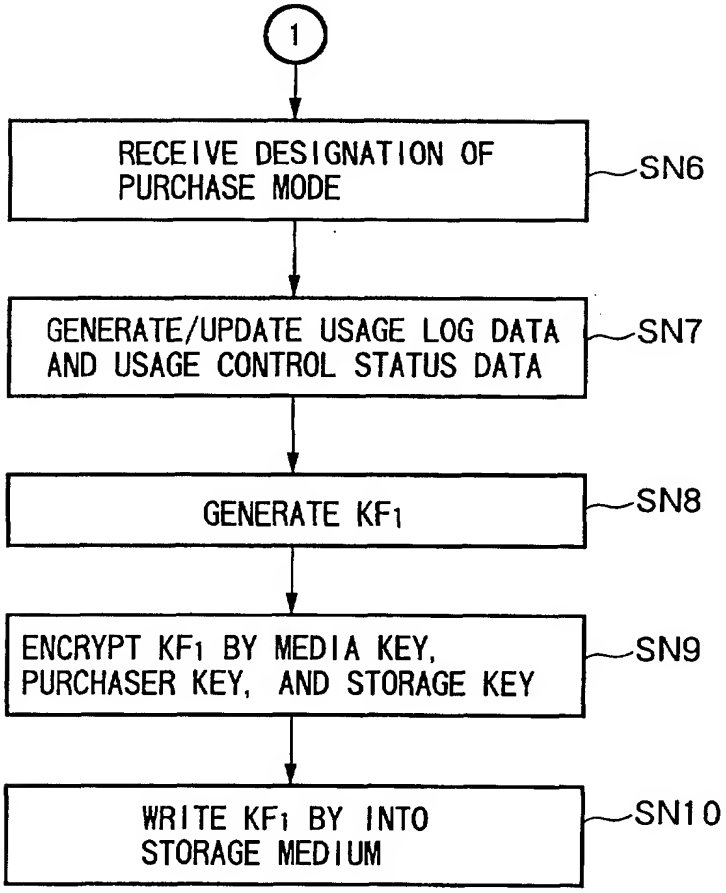
PROCESSING OF SAM 105$_3$

FIG.38



PROCESSING OF SAM 1052

FIG.39



PROCESSING OF SAM 105_2

FIG.40

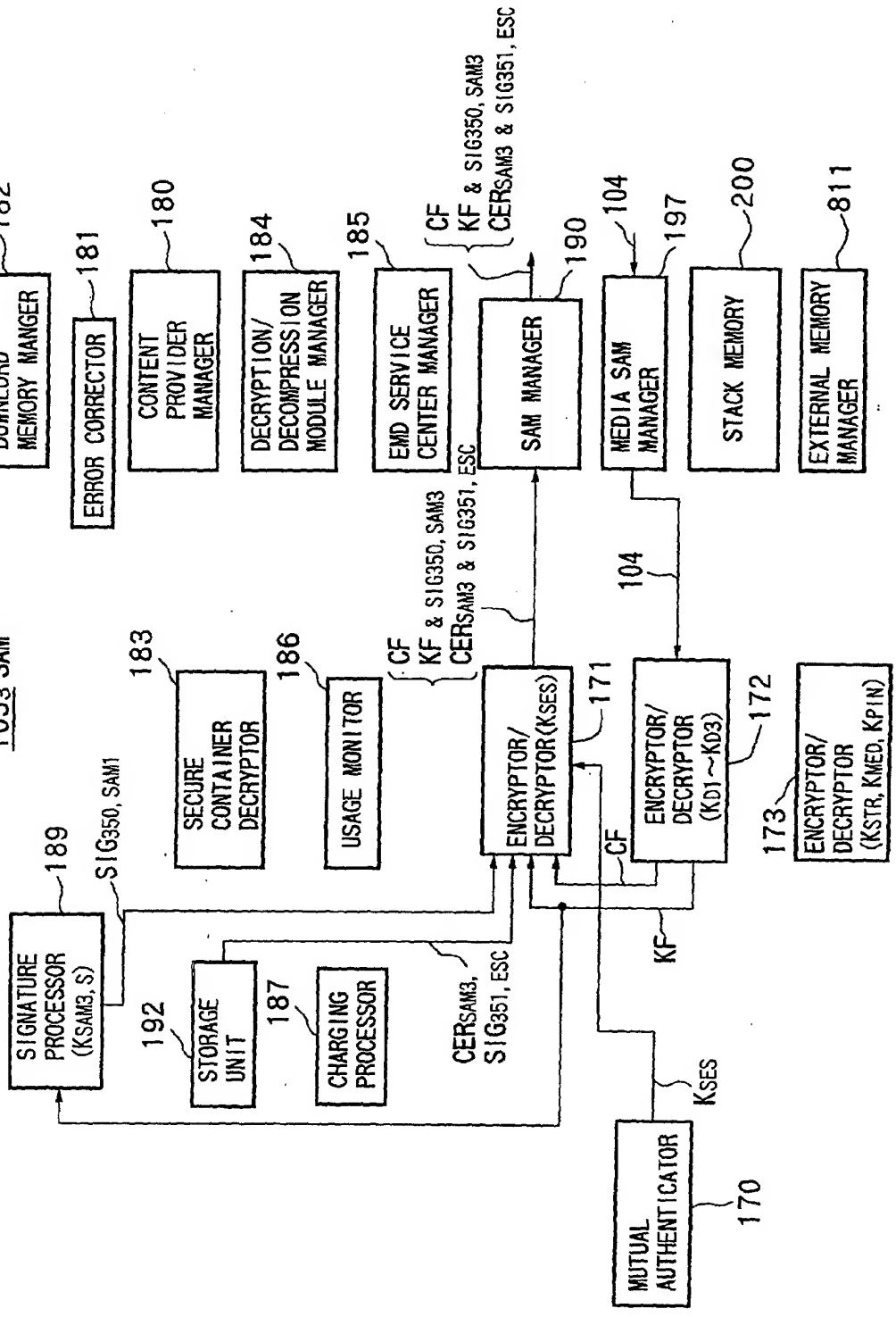

105₃ SAM
DOWNLORD MEMORY MANGER
182
ERROR CORRECTOR
181
CONTENT PROVIDER MANAGER
180
DECRYPTION/ DECOMPRESSION MODULE MANAGER
184
EMD SERVICE CENTER MANAGER
185
CF
KF & SIG350, SAM3
CERSAM3 & SIG351, ESC
SAM MANAGER
190
MEDIA SAM MANAGER
104
197
STACK MEMORY
200
EXTERNAL MEMORY MANAGER
811
SECURE CONTAINER DECRYPTOR
183
USAGE MONITOR
186
CF
KF & SIG350, SAM3
CERSAM3 & SIG351, ESC
ENCRYPTOR/ DECRYPTOR(KSES)
171
ENCRYPTOR/ DECRYPTOR (KD1~KD3)
172
104
ENCRYPTOR/ DECRYPTOR (KSTR, KMED, KPIN)
173
SIGNATURE PROCESSOR (KSAM3, S)
189
SIG350, SAM1
STORAGE UNIT
192
CHARGING PROCESSOR
187
CERSAM3, SIG351, ESC
CF
KF
KSES
MUTUAL AUTHENTICATOR
170

FIG.41

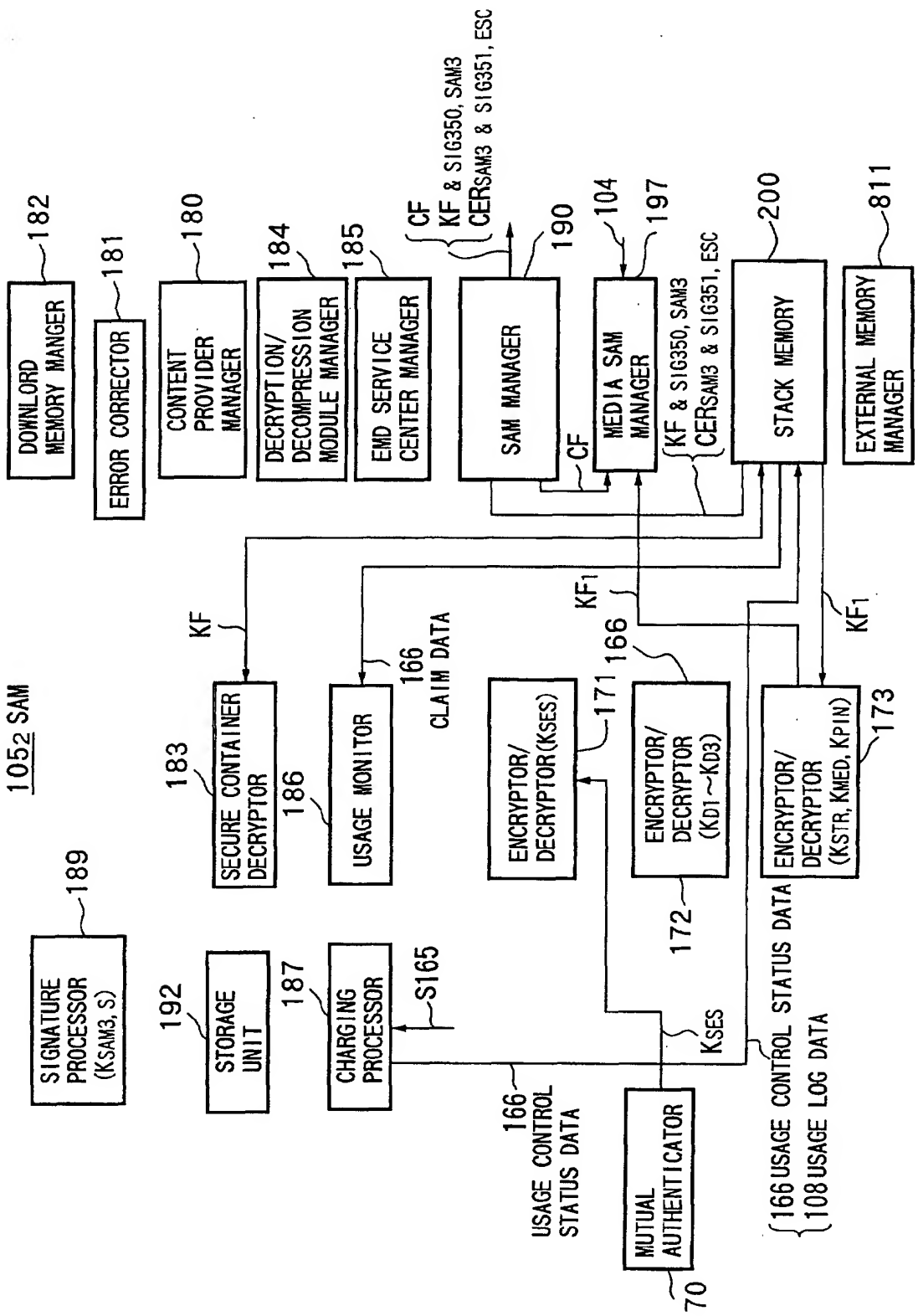

105₂ SAM
SIGNATURE PROCESSOR (KSAM3, S)
189
STORAGE UNIT
192
CHARGING PROCESSOR
187
S165
SECURE CONTAINER DECRYPTOR
183
USAGE MONITOR
186
166 CLAIM DATA
KF
ENCRYPTOR/ DECRYPTOR(KSES)
171
ENCRYPTOR/ DECRYPTOR (KD1~KD3)
172
166
ENCRYPTOR/ DECRYPTOR (KSTR, KMED, KPIN)
173
KF1
KF1
MUTUAL AUTHENTICATOR
170
KSES
166 USAGE CONTROL STATUS DATA
166 USAGE CONTROL STATUS DATA
108 USAGE LOG DATA
DOWNLORD MEMORY MANGER
182
ERROR CORRECTOR
181
CONTENT PROVIDER MANAGER
180
DECRYPTION/ DECOMPRESSION MODULE MANAGER
184
EMD SERVICE CENTER MANAGER
185
CF
KF & SIG350, SAM3
CERSAM3 & SIG351, ESC
SAM MANAGER
190
CF
MEDIA SAM MANAGER
104
KF & SIG350, SAM3
CERSAM3 & SIG351, ESC
197
STACK MEMORY
200
EXTERNAL MEMORY MANAGER
811

FIG.42A 101(CP)→SAM105$_1$ (IN BAND)

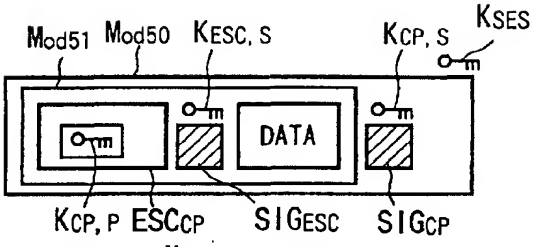


FIG.42B 101(CP)→SAM105$_1$ (OUT OF BAND)

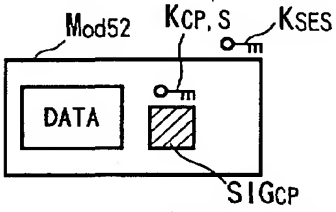


FIG.42C 102(ESC)→SAM105$_1$ (OUT OF BAND)

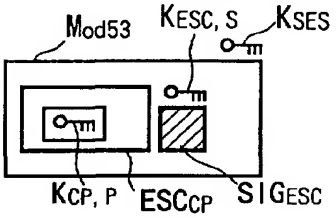


FIG.42D SAM105$_1$→101(CP) (IN BAND)

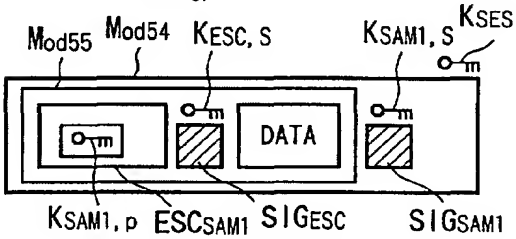


FIG.42E SAM105$_1$→101(CP) (OUT OF BAND)

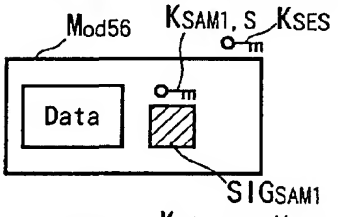


FIG.42F 102(ESC)→101(CP) (OUT OF BAND)

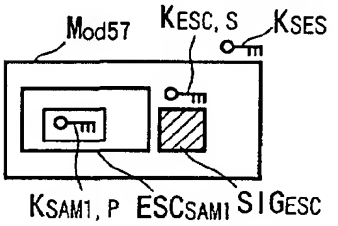


FIG.43A 101(CP)→102(ESC) (IN BAND)

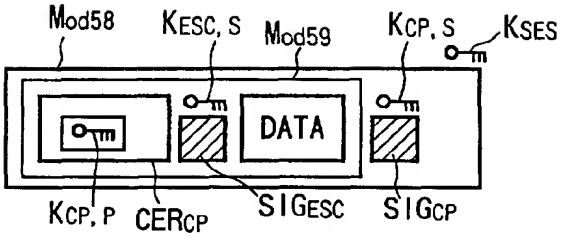


FIG.43B 101(CP)→102(ESC) (OUT OF BAND)

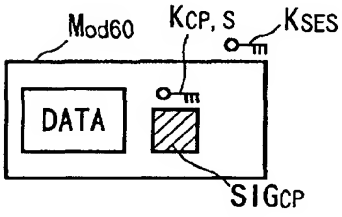


FIG.43C SAM1051→102(ESC) (IN BAND)

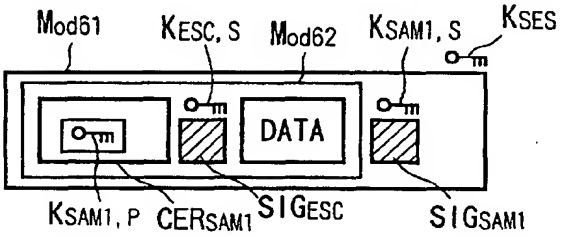


FIG.43D SAM1051→102(ESC) (OUT OF BAND)

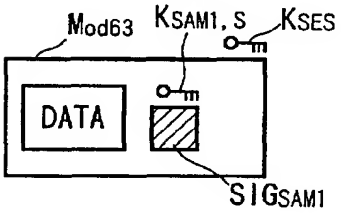


FIG.44

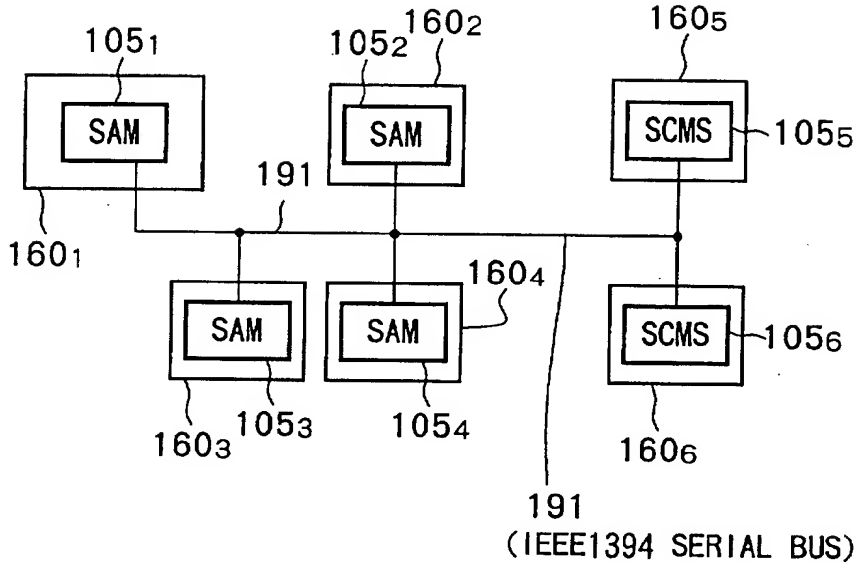
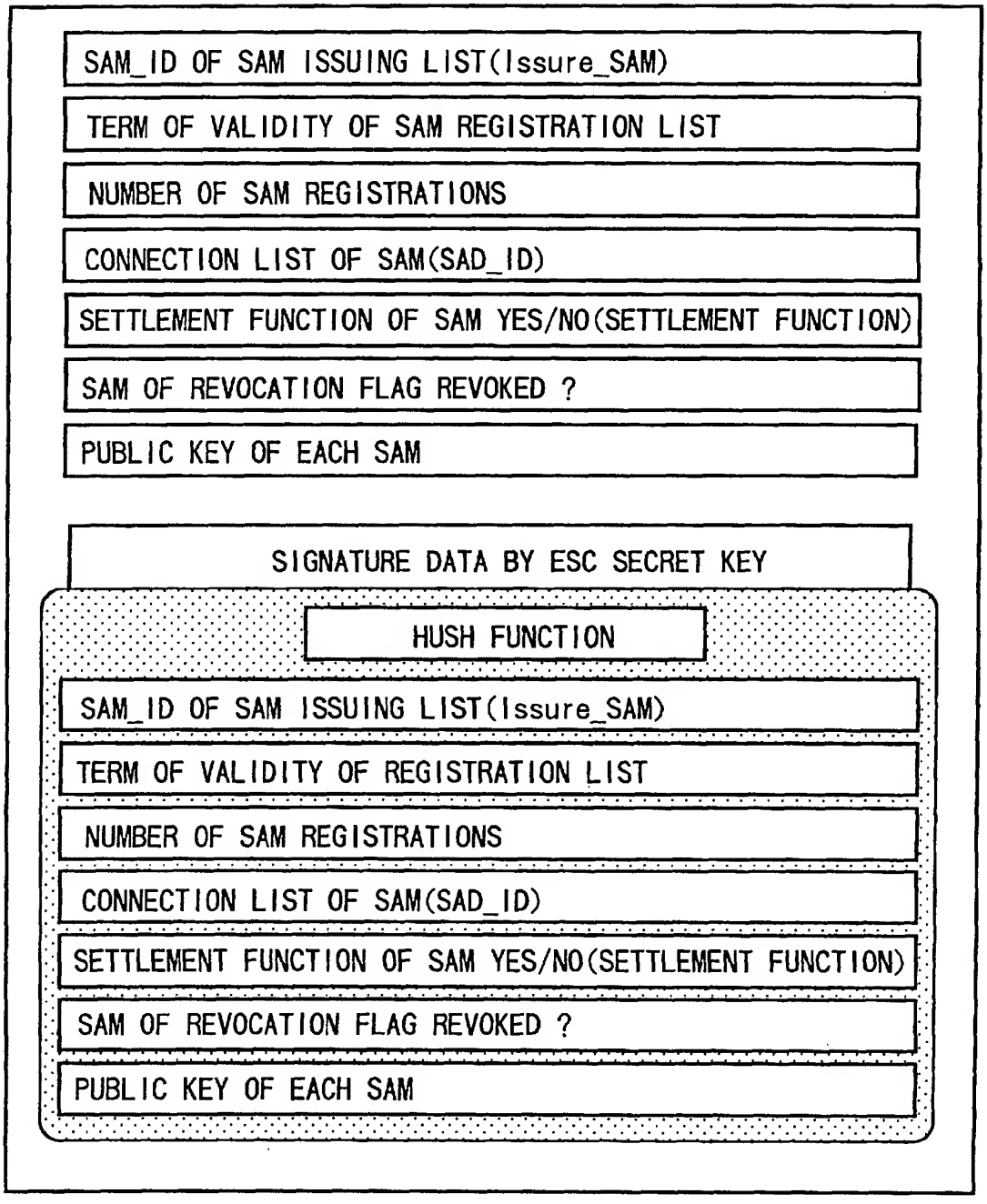

1051
1052
1602
1605
SAM
SAM
SCMS
1055
191
1601
1604
SAM
SAM
SCMS
1056
1603
1053
1054
1606
191
(IEEE1394 SERIAL BUS)

FIG.45



SAM REGISTRATION LIST

FIG.46

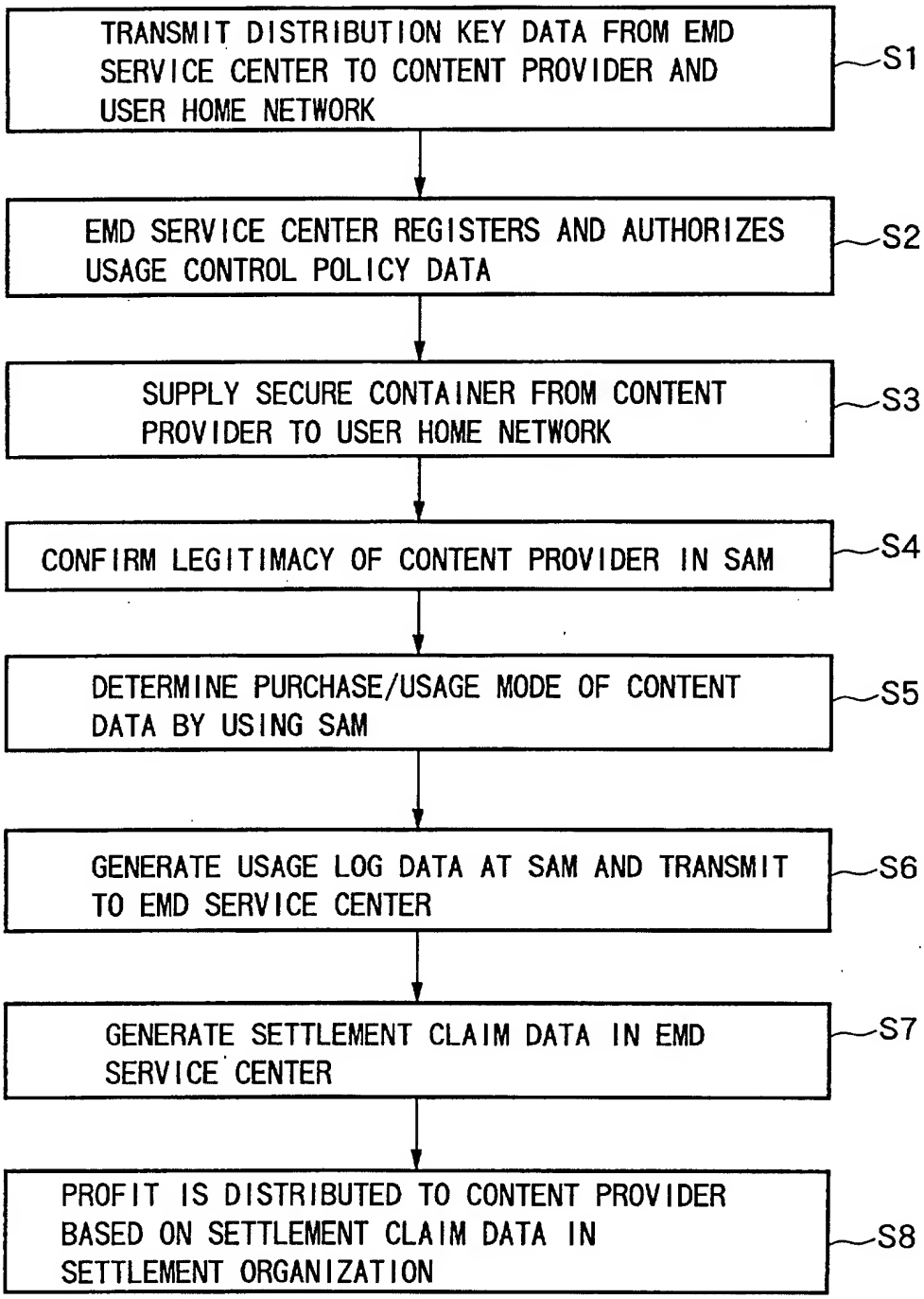

TRANSMIT DISTRIBUTION KEY DATA FROM EMD SERVICE CENTER TO CONTENT PROVIDER AND USER HOME NETWORK
S1
EMD SERVICE CENTER REGISTERS AND AUTHORIZES USAGE CONTROL POLICY DATA
S2
SUPPLY SECURE CONTAINER FROM CONTENT PROVIDER TO USER HOME NETWORK
S3
CONFIRM LEGITIMACY OF CONTENT PROVIDER IN SAM
S4
DETERMINE PURCHASE/USAGE MODE OF CONTENT DATA BY USING SAM
S5
GENERATE USAGE LOG DATA AT SAM AND TRANSMIT TO EMD SERVICE CENTER
S6
GENERATE SETTLEMENT CLAIM DATA IN EMD SERVICE CENTER
S7
PROFIT IS DISTRIBUTED TO CONTENT PROVIDER BASED ON SETTLEMENT CLAIM DATA IN SETTLEMENT ORGANIZATION
S8

FIG.47

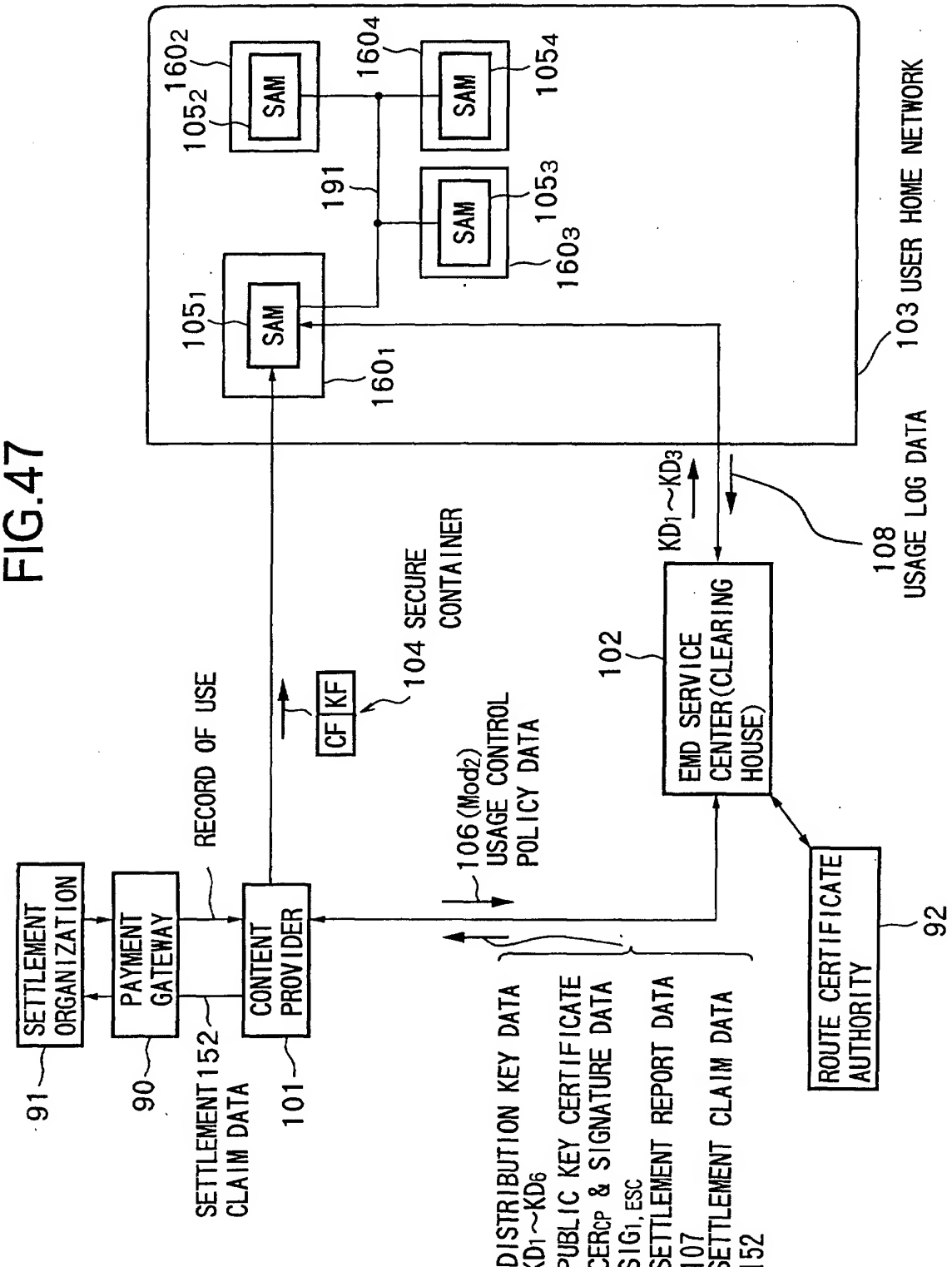

SETTLEMENT ORGANIZATION
91
PAYMENT GATEWAY
90
CONTENT PROVIDER
101
RECORD OF USE
SETTLEMENT 152
CLAIM DATA
CF KF
104 SECURE CONTAINER
106(Mod2)
USAGE CONTROL
POLICY DATA
EMD SERVICE CENTER(CLEARING HOUSE)
102
ROUTE CERTIFICATE AUTHORITY
92
KD1~KD3
108
USAGE LOG DATA
103 USER HOME NETWORK
SAM
1051
1601
1052
1602
191
1603
1053
1604
1054
•DISTRIBUTION KEY DATA
KD1~KD6
•PUBLIC KEY CERTIFICATE
CERCP & SIGNATURE DATA
SIG1, ESC
•SETTLEMENT REPORT DATA
107
•SETTLEMENT CLAIM DATA
152

FIG.48

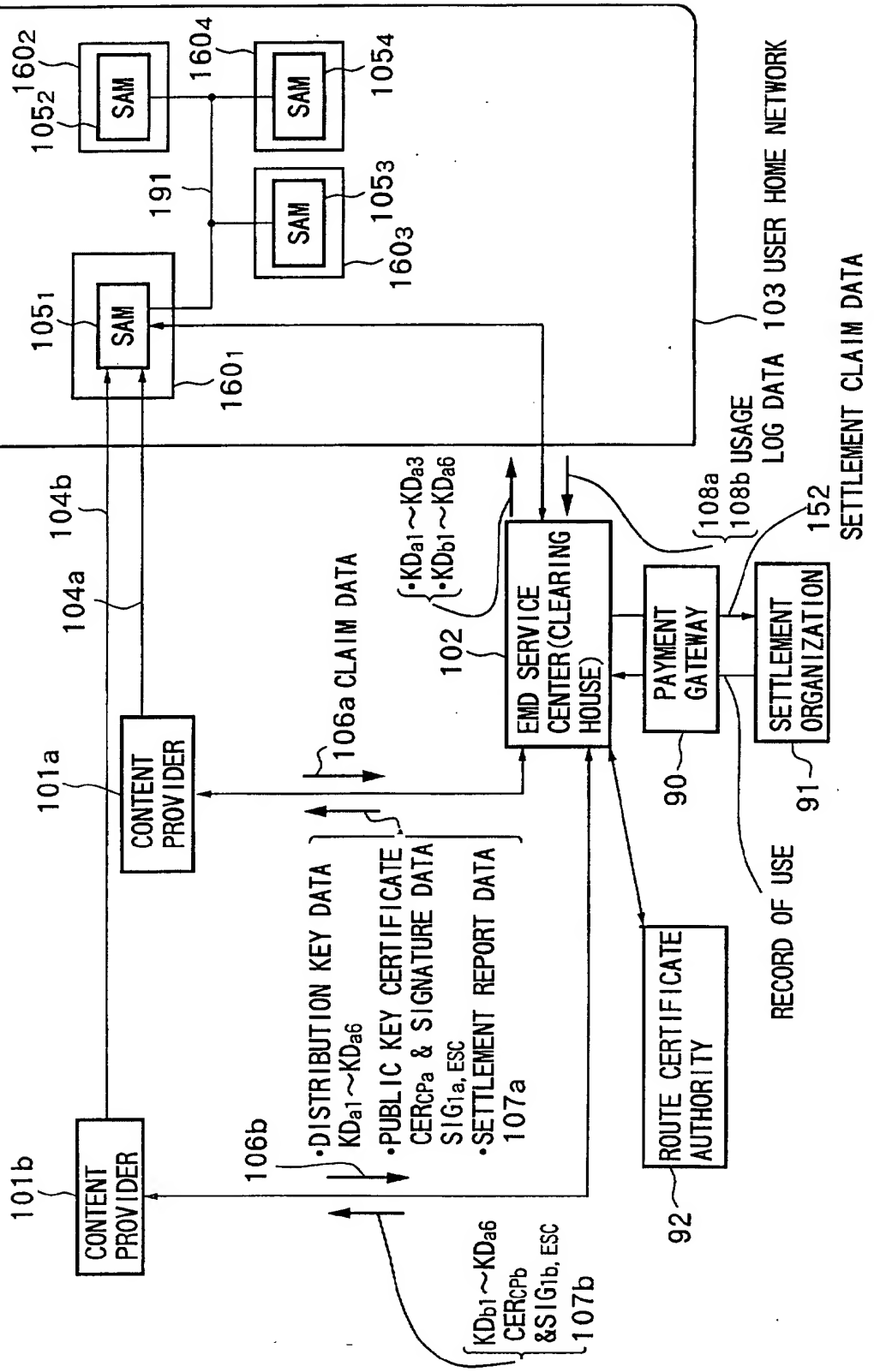

SAM
SAM
SAM
SAM
191
103 USER HOME NETWORK
CONTENT PROVIDER
CONTENT PROVIDER
EMD SERVICE CENTER(CLEARING HOUSE)
PAYMENT GATEWAY
SETTLEMENT ORGANIZATION
ROUTE CERTIFICATE AUTHORITY
106a CLAIM DATA
106b
•DISTRIBUTION KEY DATA KDa1~KDa6
•PUBLIC KEY CERTIFICATE CERCPa & SIGNATURE DATA SIG1a, ESC
•SETTLEMENT REPORT DATA 107a
KDb1~KDa6 CERCPb &SIG1b, ESC 107b
•KDa1~KDa3 •KDb1~KDa6
108a USAGE LOG DATA
108b SETTLEMENT CLAIM DATA
RECORD OF USE
90
91
92
102
152

FIG.49

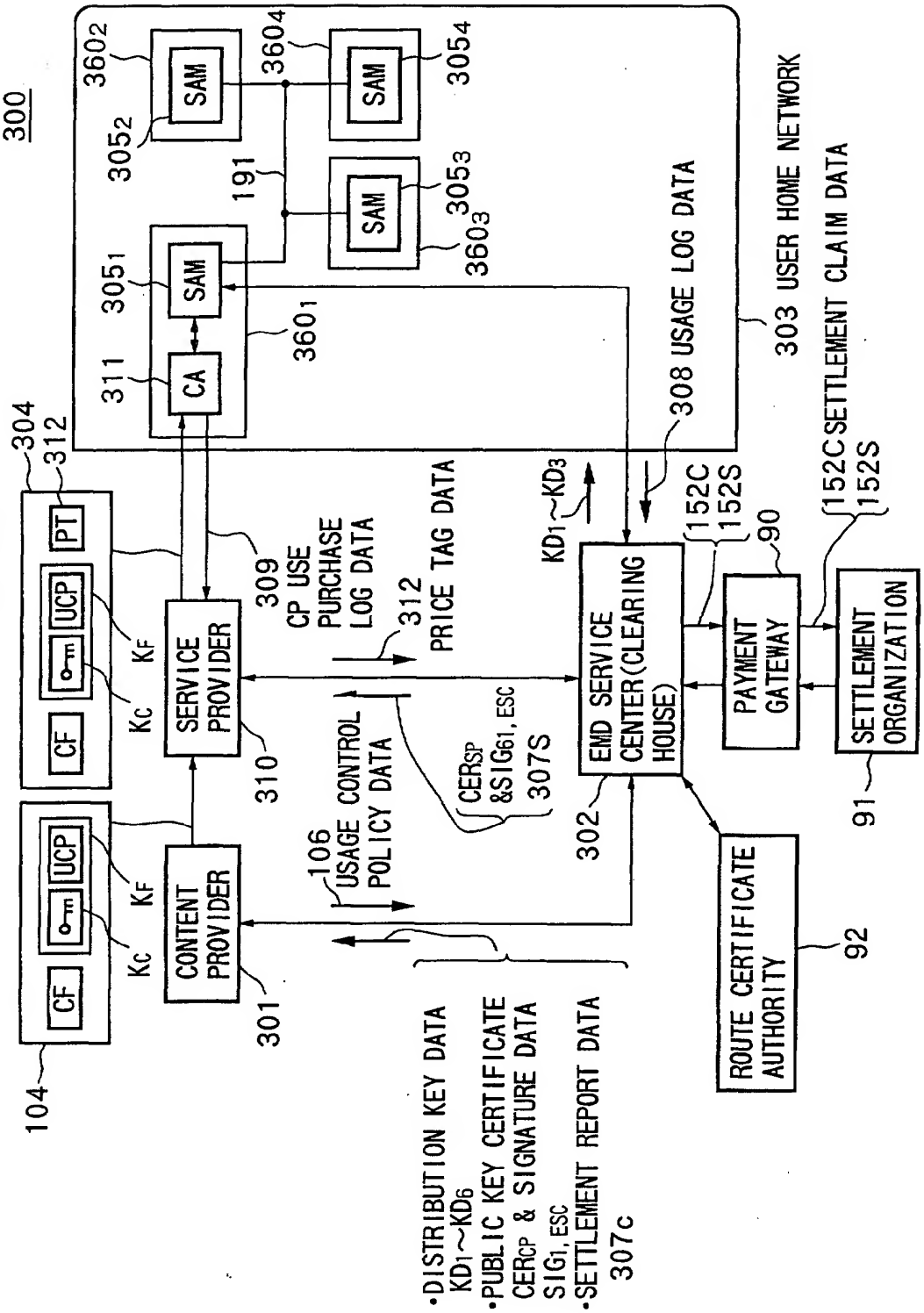

300
303 USER HOME NETWORK
SAM
CA
CF
UCP
PT
SERVICE PROVIDER
CONTENT PROVIDER
EMD SERVICE CENTER(CLEARING HOUSE)
PAYMENT GATEWAY
SETTLEMENT ORGANIZATION
ROUTE CERTIFICATE AUTHORITY
308 USAGE LOG DATA
309 CP USE PURCHASE LOG DATA
312 PRICE TAG DATA
106 USAGE CONTROL POLICY DATA
152C SETTLEMENT CLAIM DATA
•DISTRIBUTION KEY DATA KD1~KD6
•PUBLIC KEY CERTIFICATE CERCP & SIGNATURE DATA SIG1, ESC
•SETTLEMENT REPORT DATA 307c

FIG.50

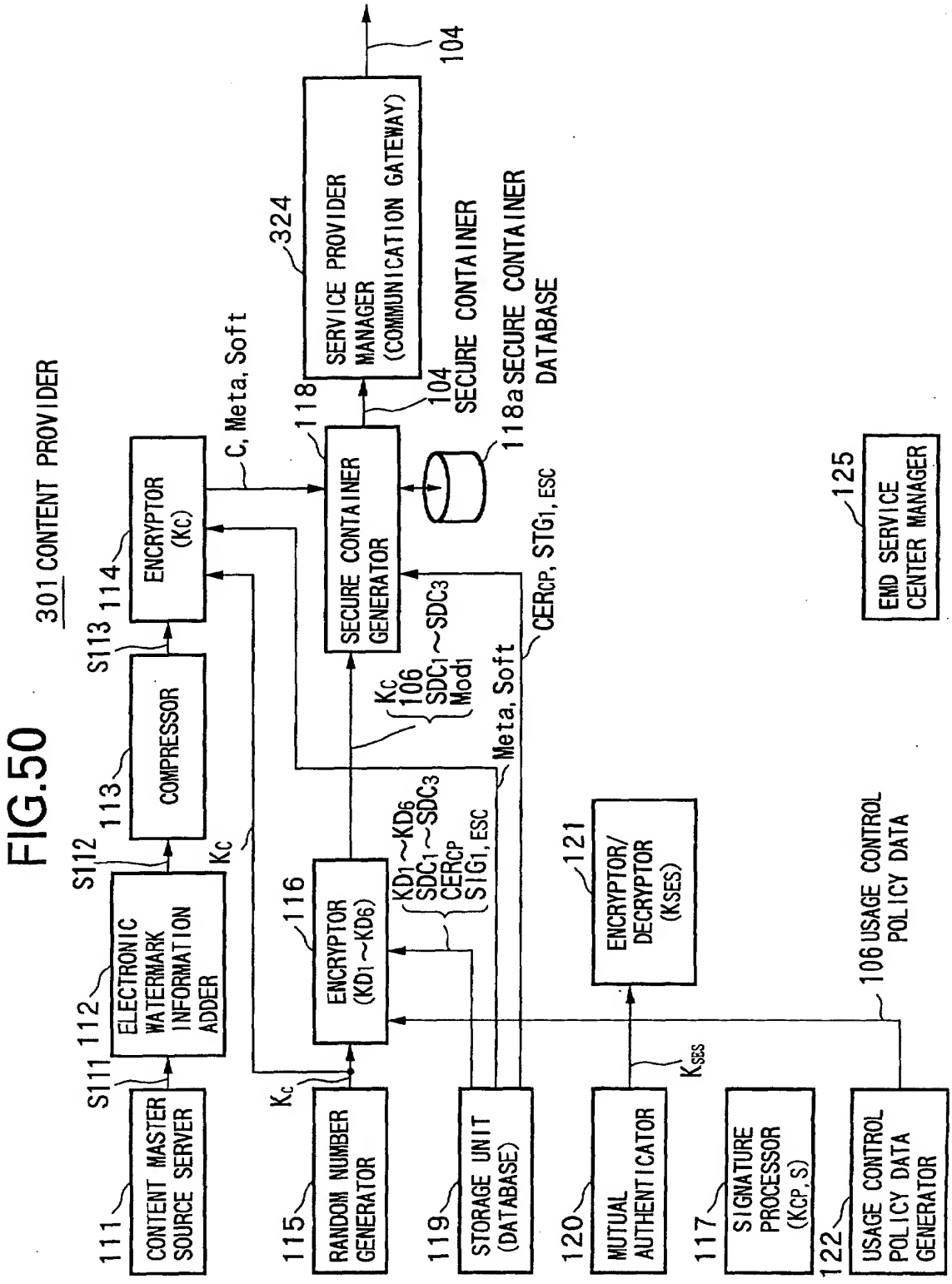

301 CONTENT PROVIDER
111 CONTENT MASTER SOURCE SERVER
S111
112 ELECTRONIC WATERMARK INFORMATION ADDER
S112
113 COMPRESSOR
S113
114 ENCRYPTOR (Kc)
C, Meta, Soft
324 SERVICE PROVIDER MANAGER (COMMUNICATION GATEWAY)
104
104 SECURE CONTAINER
118a SECURE CONTAINER DATABASE
118 SECURE CONTAINER GENERATOR
Kc
106
SDC1~SDC3
Mod1
Meta, Soft
CERCP, STG1, ESC
115 RANDOM NUMBER GENERATOR
Kc
116 ENCRYPTOR (KD1~KD6)
KD1~KD6
SDC1~SDC3
CERCP
STG1, ESC
119 STORAGE UNIT (DATABASE)
121 ENCRYPTOR/ DECRYPTOR (KSES)
KSES
120 MUTUAL AUTHENTICATOR
117 SIGNATURE PROCESSOR (KCP, S)
122 USAGE CONTROL POLICY DATA GENERATOR
106 USAGE CONTROL POLICY DATA
125 EMD SERVICE CENTER MANAGER

FIG.51

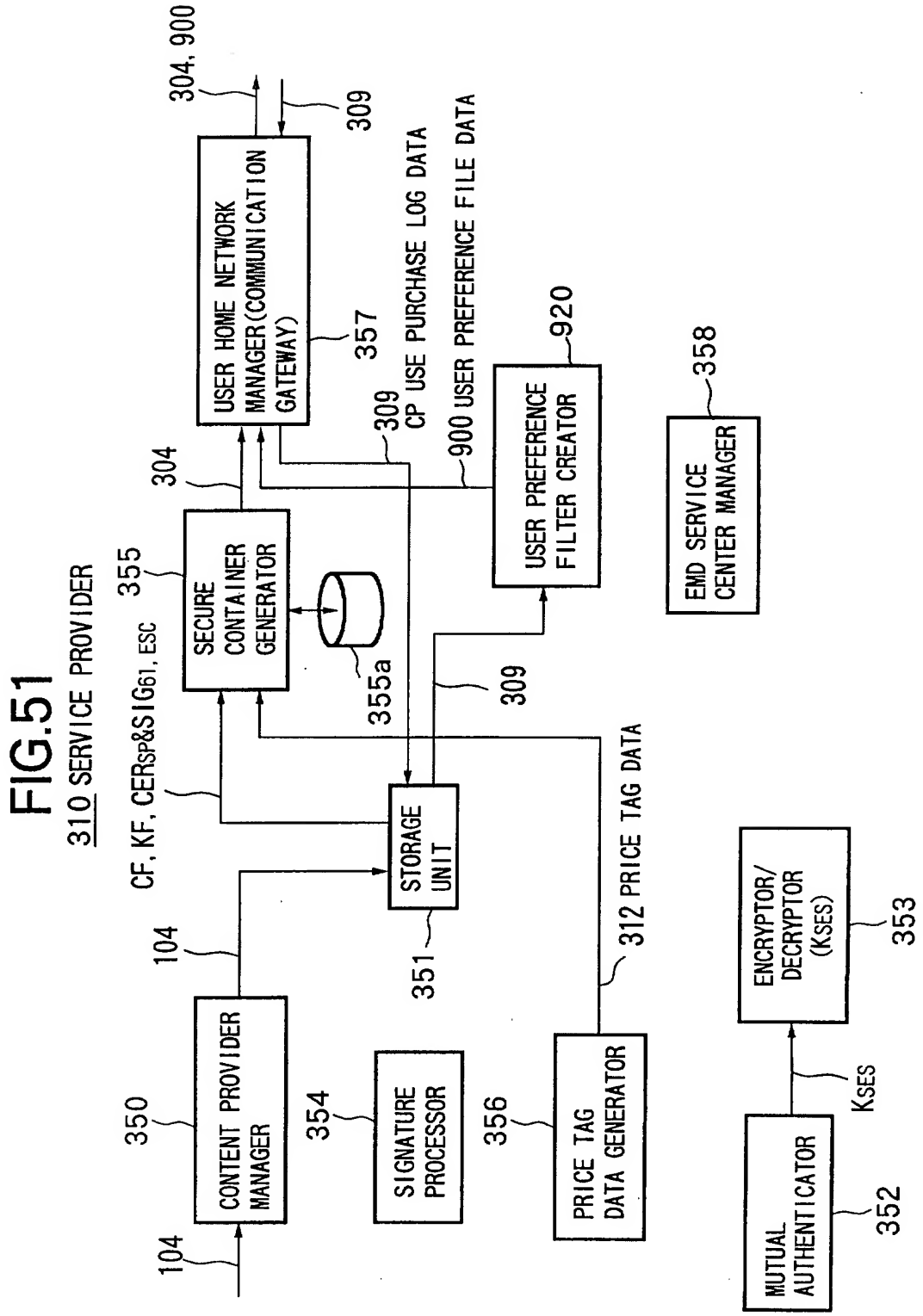
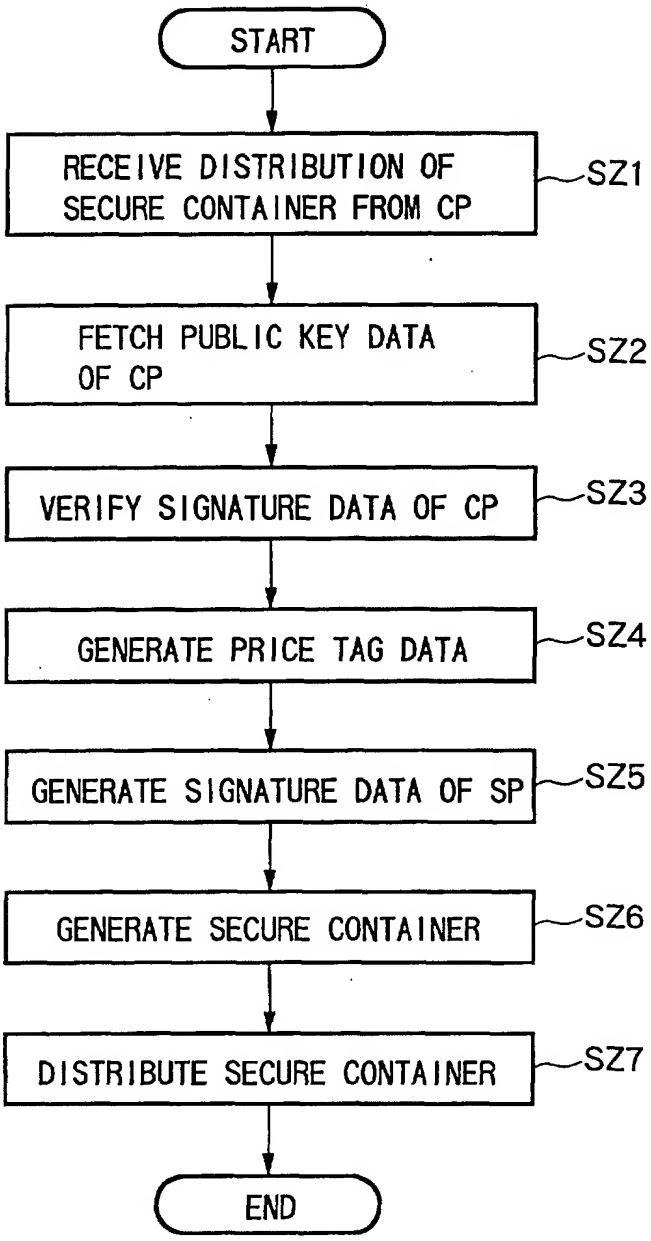

310 SERVICE PROVIDER
CONTENT PROVIDER MANAGER
350
104
104
SIGNATURE PROCESSOR
354
STORAGE UNIT
351
CF, KF, CERSP&SIG61, ESC
SECURE CONTAINER GENERATOR
355
355a
304
304, 900
USER HOME NETWORK MANAGER(COMMUNICATION GATEWAY)
357
309
309
CP USE PURCHASE LOG DATA
900 USER PREFERENCE FILE DATA
USER PREFERENCE FILTER CREATOR
920
309
312 PRICE TAG DATA
PRICE TAG DATA GENERATOR
356
EMD SERVICE CENTER MANAGER
358
ENCRYPTOR/ DECRYPTOR (KSES)
353
KSES
MUTUAL AUTHENTICATOR
352

FIG.52


START
RECEIVE DISTRIBUTION OF SECURE CONTAINER FROM CP
SZ1
FETCH PUBLIC KEY DATA OF CP
SZ2
VERIFY SIGNATURE DATA OF CP
SZ3
GENERATE PRICE TAG DATA
SZ4
GENERATE SIGNATURE DATA OF SP
SZ5
GENERATE SECURE CONTAINER
SZ6
DISTRIBUTE SECURE CONTAINER
SZ7
END

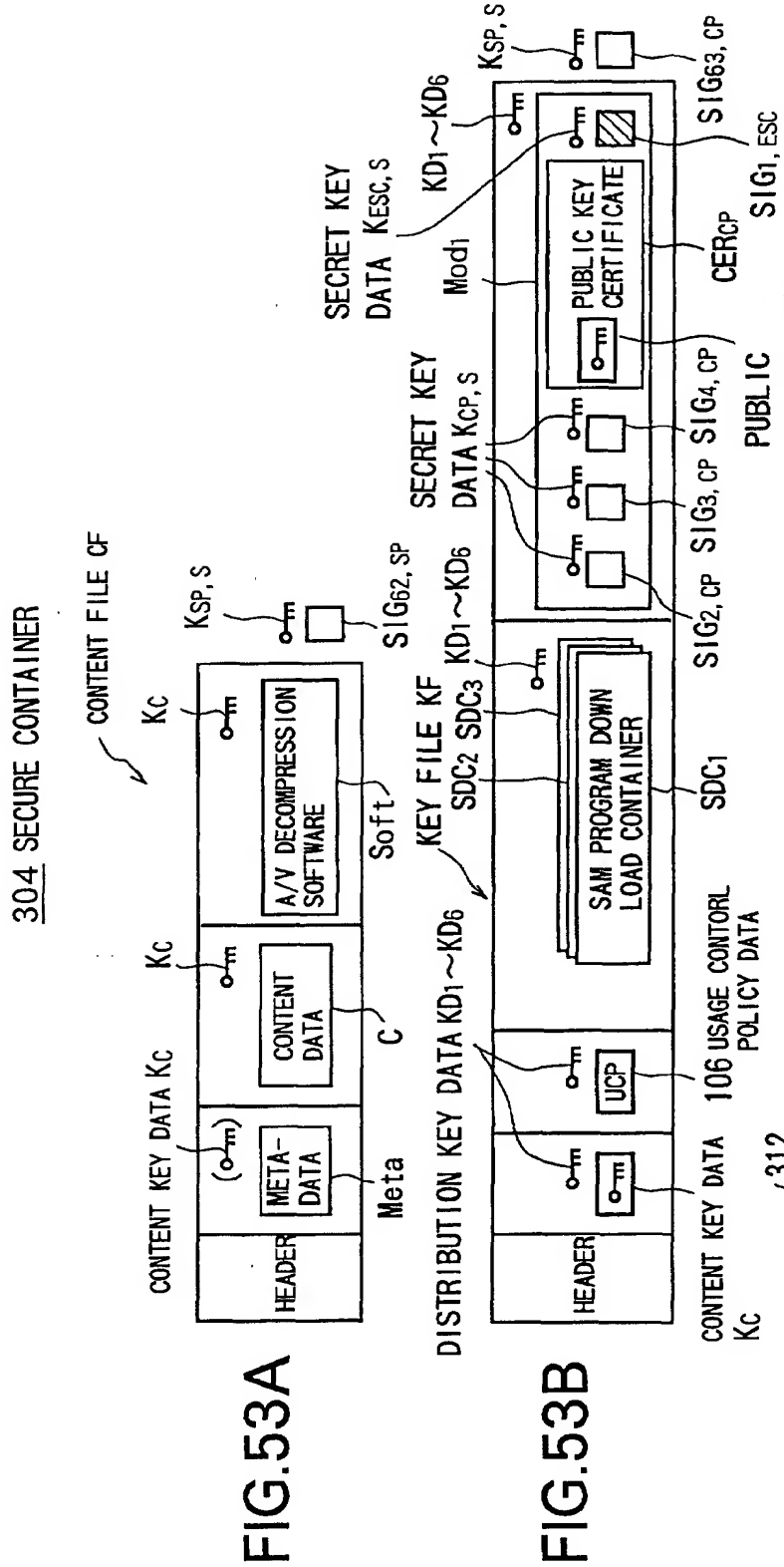


FIG.53A

FIG.53B

FIG.53C

FIG.53D

FIG.54

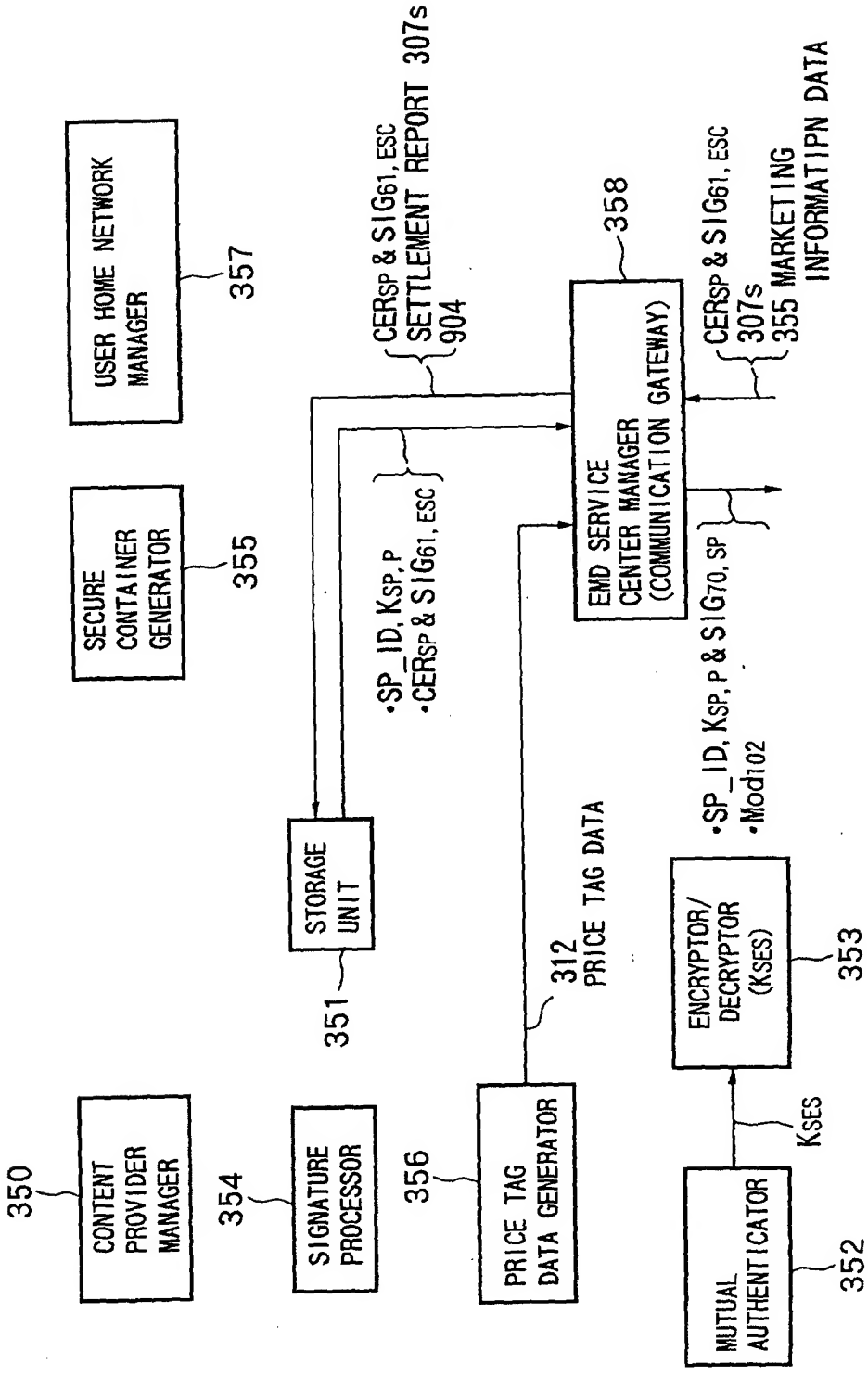

310 SERVICE PROVIDER
CONTENT PROVIDER MANAGER
350
SIGNATURE PROCESSOR
354
PRICE TAG DATA GENERATOR
356
STORAGE UNIT
351
SECURE CONTAINER GENERATOR
355
USER HOME NETWORK MANAGER
357
312 PRICE TAG DATA
•SP_ID, KSP, P
•CERSP & SIG61, ESC
CERSP & SIG61, ESC SETTLEMENT REPORT 307s 904
EMD SERVICE CENTER MANAGER (COMMUNICATION GATEWAY)
358
CERSP & SIG61, ESC 307s
355 MARKETING INFORMATIPN DATA
•SP_ID, KSP, P & SIG70, SP
•Mod102
ENCRYPTOR/ DECRYPTOR (KSES)
353
KSES
MUTUAL AUTHENTICATOR
352

FIG.55

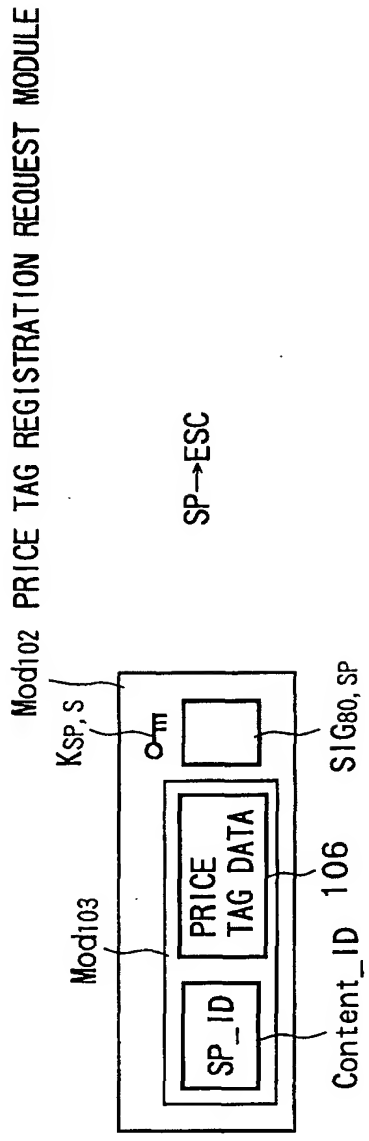

Mod102 PRICE TAG REGISTRATION REQUEST MODULE
SP→ESC
KSP, S
SIG80, SP
Mod103
PRICE TAG DATA
SP_ID
Content_ID 106

FIG.56

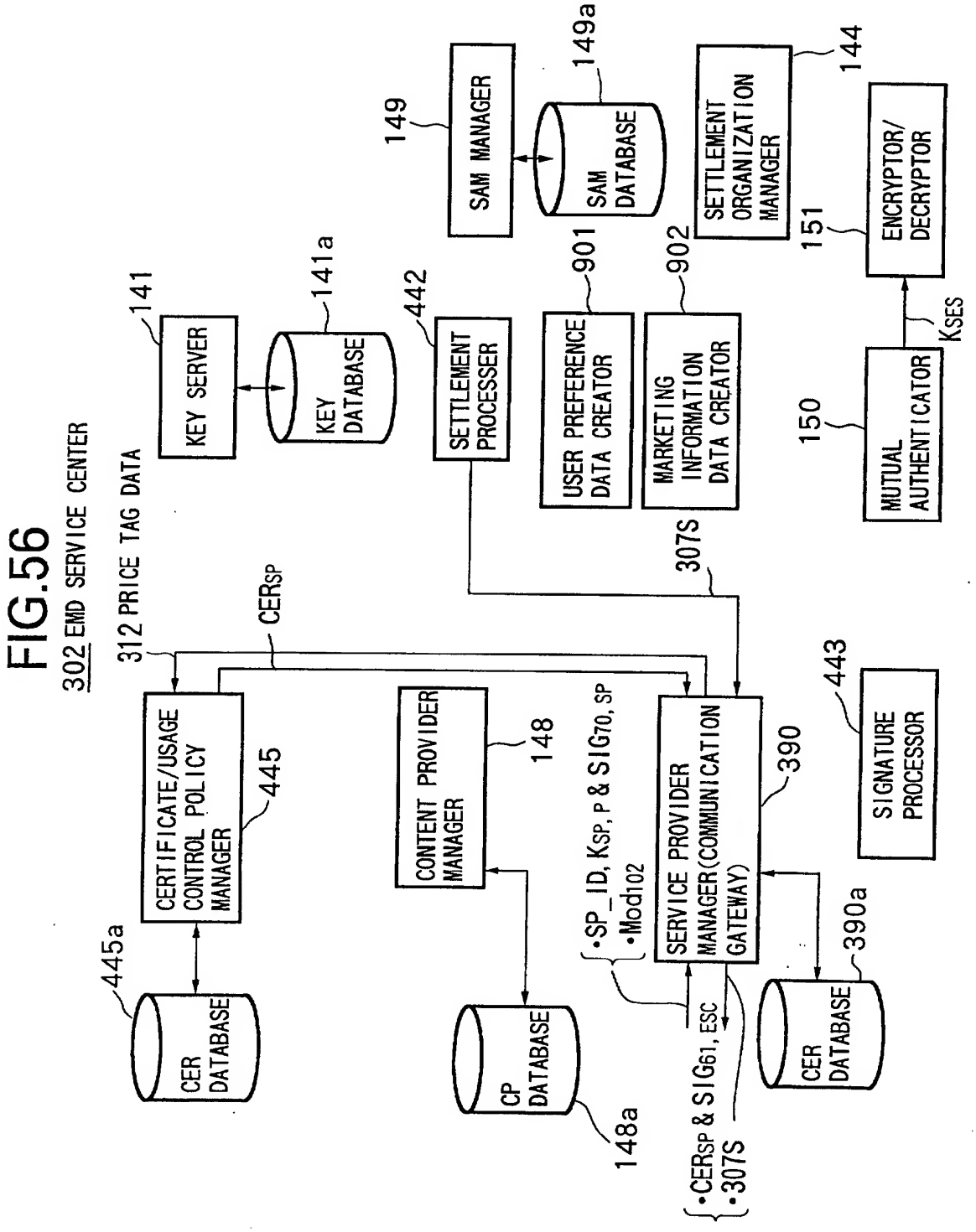

302 EMD SERVICE CENTER
312 PRICE TAG DATA
141
KEY SERVER
141a
KEY DATABASE
442
SETTLEMENT PROCESSER
149
SAM MANAGER
149a
SAM DATABASE
901
USER PREFERENCE DATA CREATOR
902
MARKETING INFORMATION DATA CREATOR
144
SETTLEMENT ORGANIZATION MANAGER
151
ENCRYPTOR/ DECRYPTOR
150
MUTUAL AUTHENTICATOR
KSES
307S
CERSP
CERTIFICATE/USAGE CONTROL POLICY MANAGER
445
445a
CER DATABASE
CONTENT PROVIDER MANAGER
148
CP DATABASE
148a
•SP_ID, KSP, P & SIG70, SP
•Mod102
SERVICE PROVIDER MANAGER(COMMUNICATION GATEWAY)
390
390a
443
SIGNATURE PROCESSOR
•CERSP & SIG61, ESC
•307S

FIG.57

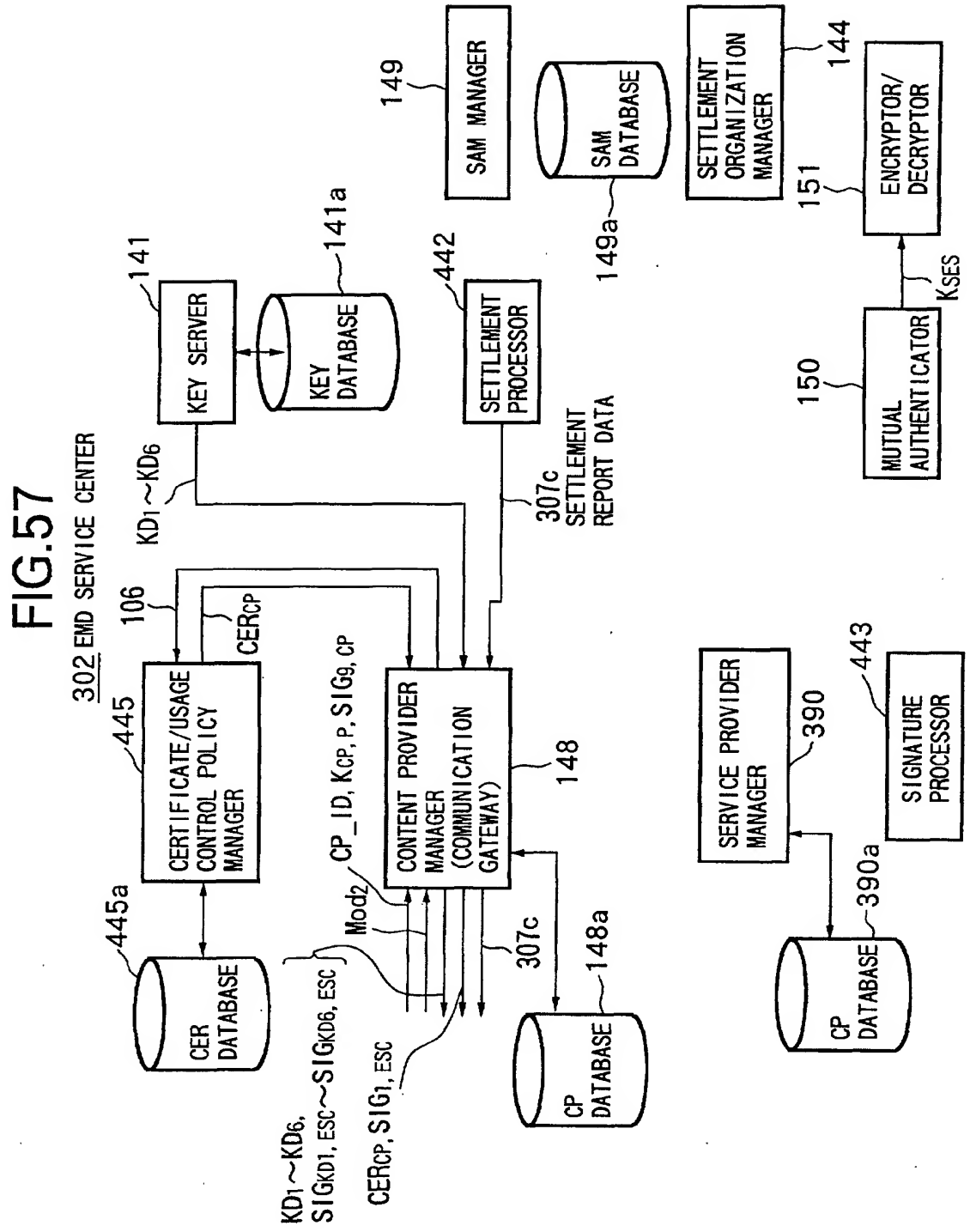

302 EMD SERVICE CENTER
106
445
CERTIFICATE/USAGE CONTROL POLICY MANAGER
CERCP
445a
CER DATABASE
141
KEY SERVER
141a
KEY DATABASE
KD1~KD6
CP_ID, KCP, P, SIG9, CP
Mod2
KD1~KD6, SIGKD1, ESC~SIGKD6, ESC
CERCP, SIG1, ESC
CONTENT PROVIDER MANAGER (COMMUNICATION GATEWAY)
148
307c
148a
CP DATABASE
442
SETTLEMENT PROCESSOR
307c SETTLEMENT REPORT DATA
149
SAM MANAGER
149a
SAM DATABASE
SERVICE PROVIDER MANAGER
390
390a
CP DATABASE
443
SIGNATURE PROCESSOR
SETTLEMENT ORGANIZATION MANAGER
144
151
ENCRYPTOR/ DECRYPTOR
KSES
150
MUTUAL AUTHENTICATOR

FIG.58

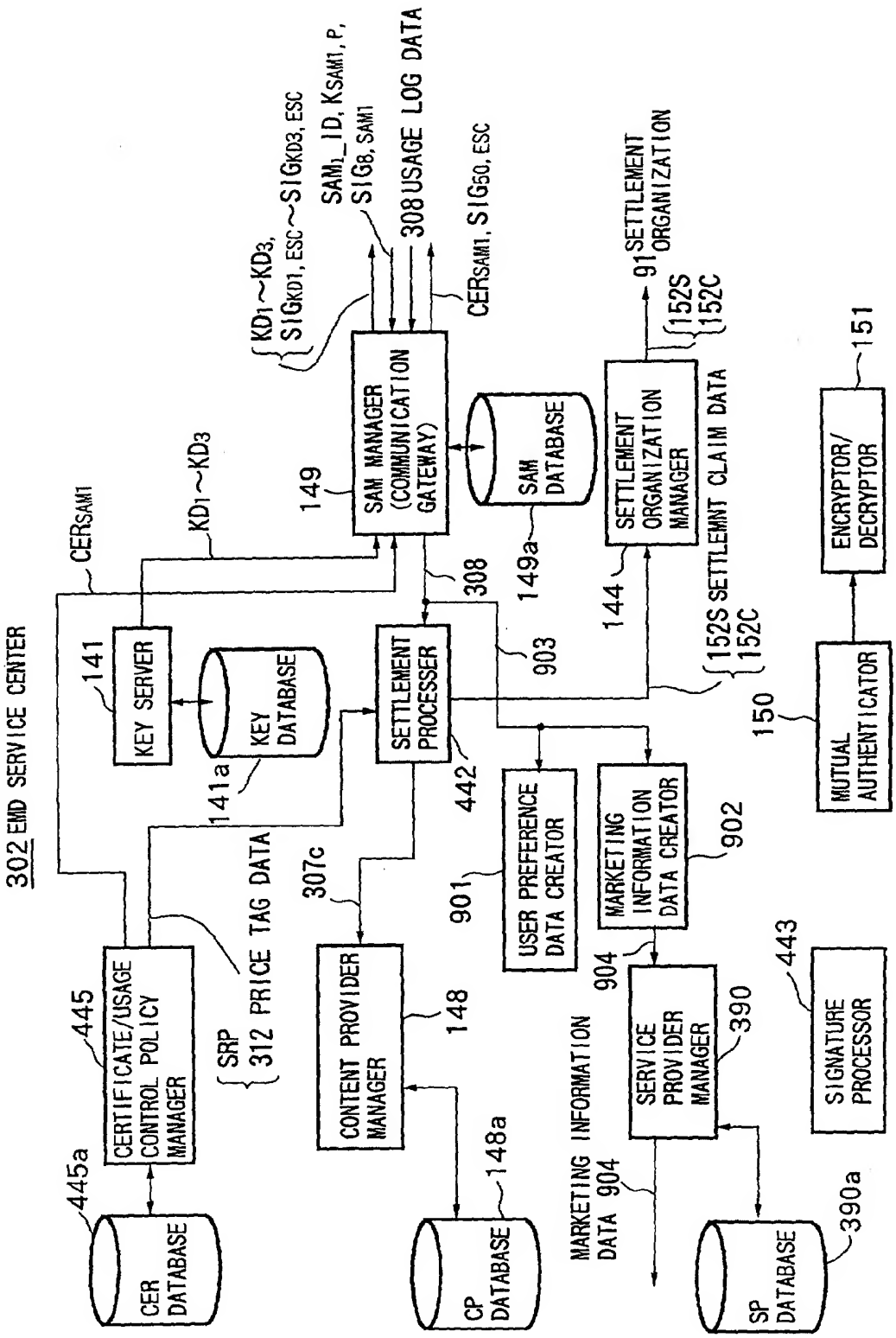
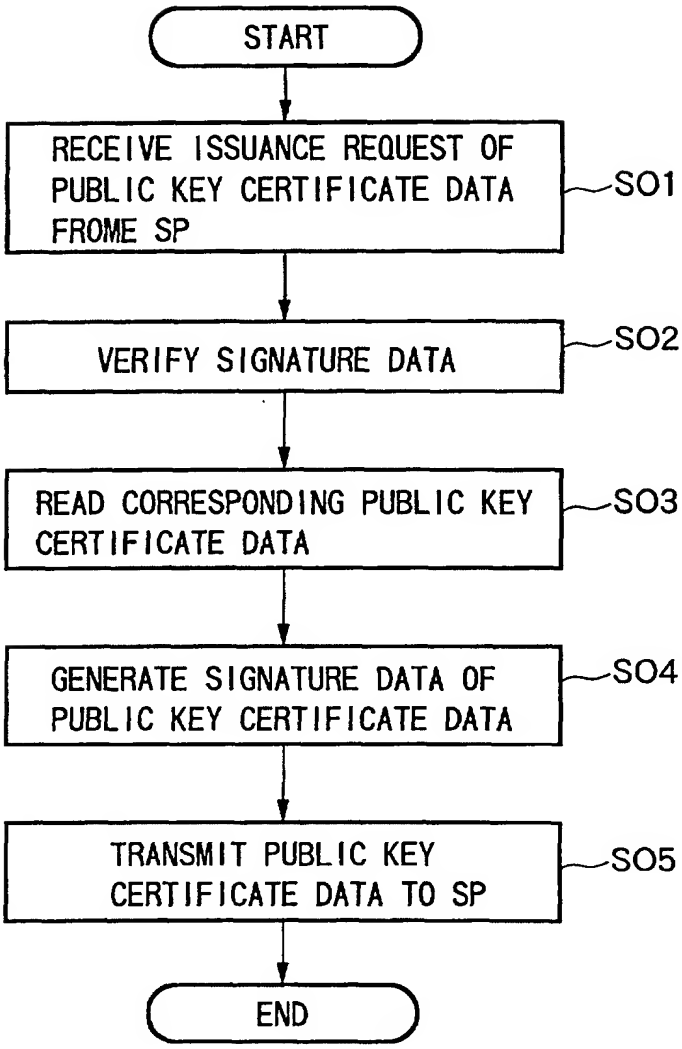

302 EMD SERVICE CENTER
CERSAM1
KD1~KD3
KD1~KD3, SIGKD1, ESC~SIGKD3, ESC
SAM1_ID, KSAM1, P, SIG8, SAM1
308 USAGE LOG DATA
CERSAM1, SIG50, ESC
91 SETTLEMENT ORGANIZATION
152S 152C
151
149
SAM MANAGER (COMMUNICATION GATEWAY)
SAM DATABASE
SETTLEMENT ORGANIZATION MANAGER
ENCRYPTOR/ DECRYPTOR
141
KEY SERVER
KEY DATABASE
141a
SETTLEMENT PROCESSER
308
903
149a
144
152S SETTLEMNT CLAIM DATA
152C
150
MUTUAL AUTHENTICATOR
442
USER PREFERENCE DATA CREATOR
MARKETING INFORMATION DATA CREATOR
902
901
307c
445
CERTIFICATE/USAGE CONTROL POLICY MANAGER
SRP
312 PRICE TAG DATA
CONTENT PROVIDER MANAGER
148
904
SERVICE PROVIDER MANAGER
390
443
SIGNATURE PROCESSOR
445a
CER DATABASE
148a
CP DATABASE
MARKETING INFORMATION DATA 904
390a
SP DATABASE

FIG.59

CONTENT OF USAGE LOG DATA 308

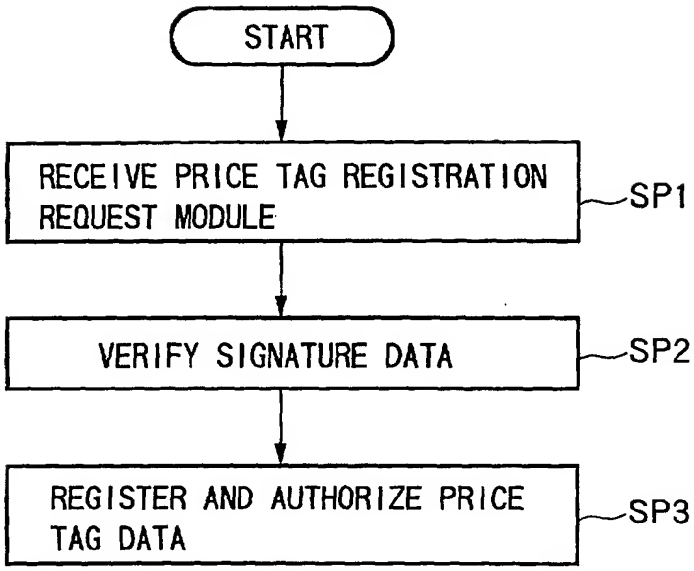
IDENTIFIER Content_ID
IDENTIFIER CP_ID
IDENTIFIER SP_ID
SIGNAL ORIGIN DATA OF CONTENT DATA C
COMPRESSION METHOD OF CONTENT DATA C
IDENTIFIER MEDIA_ID OF STORAGE MEDIUM
IDENTIFIER SAM_ID
USER_ID OF USER

FIG.60



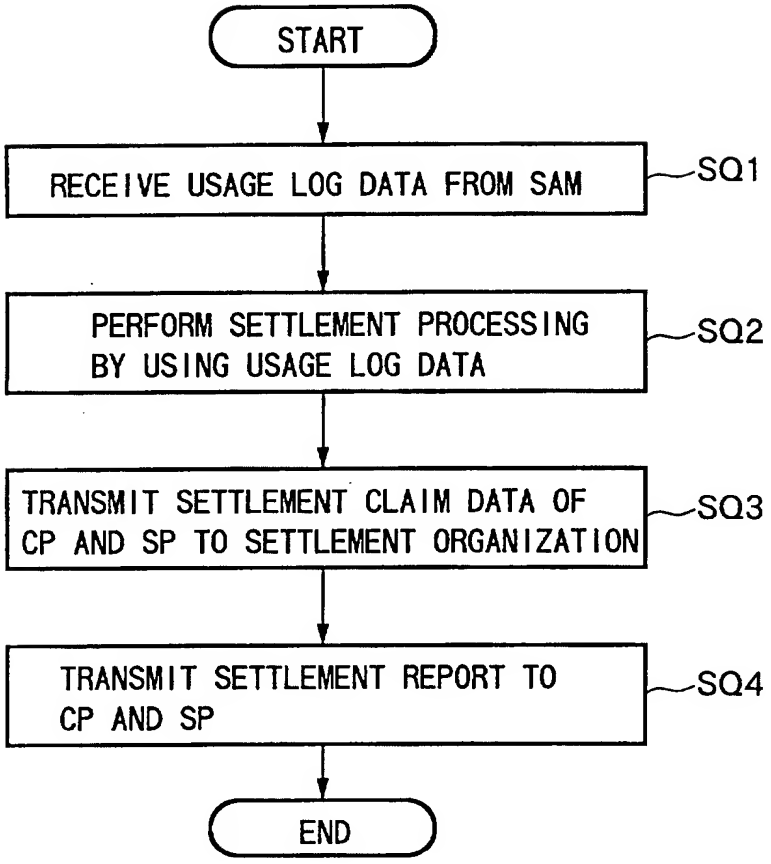
PROCESSING OF ESC IN RESPONSE TO ISSUANCE REQUEST OF PUBLIC KEY CERTIFICATE DATA FROM SP

FIG.61



PROCESSING FOR REGISTRATION OF PRICE TAG DATA IN ESC

FIG.62



PROCESSING FOR SETTLEMENT IN ESC

FIG.63

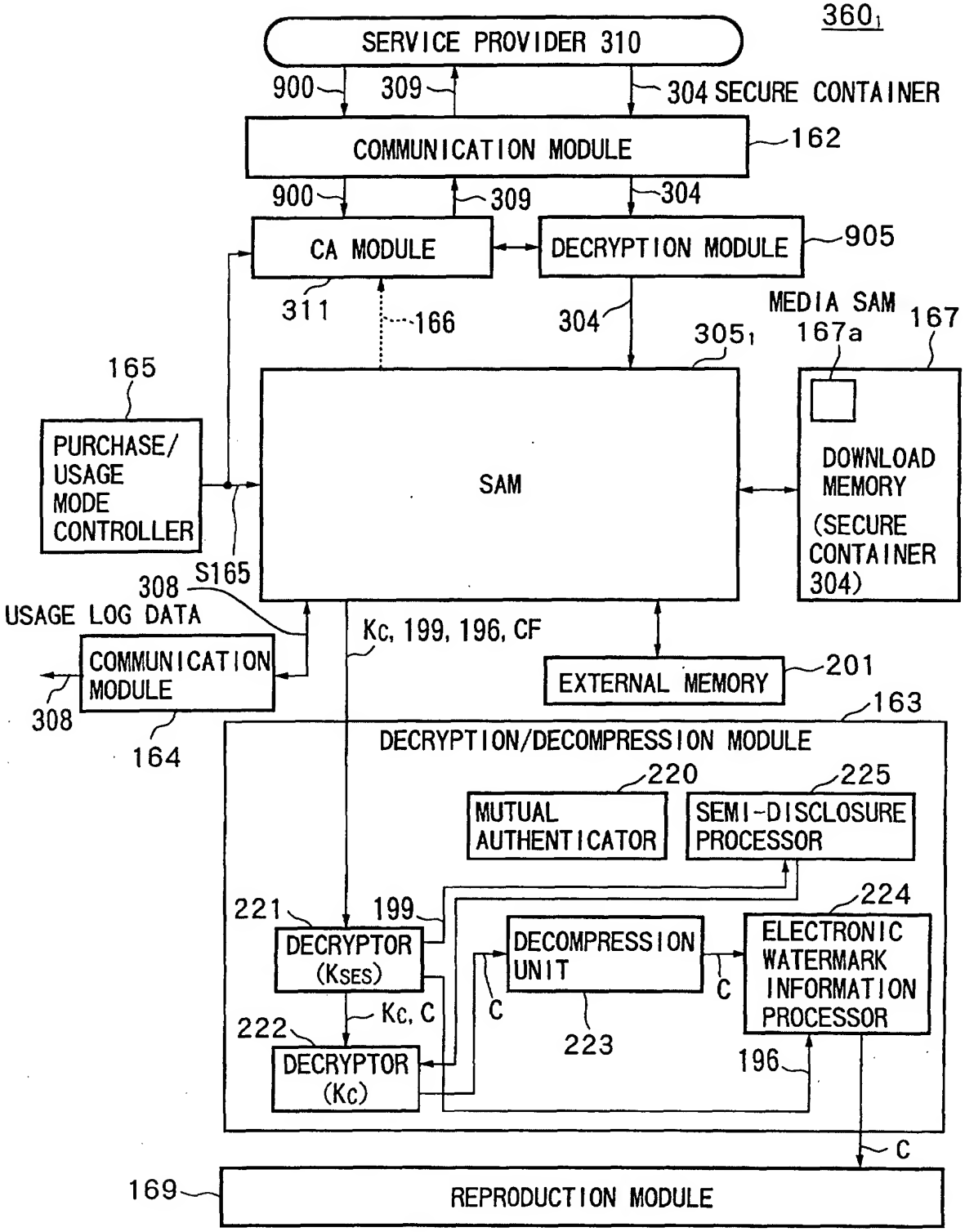

360₁
SERVICE PROVIDER 310
900
309
304 SECURE CONTAINER
COMMUNICATION MODULE
162
900
309
304
CA MODULE
DECRYPTION MODULE
905
311
166
304
MEDIA SAM
167a
167
305₁
165
PURCHASE/ USAGE MODE CONTROLLER
SAM
DOWNLOAD MEMORY (SECURE CONTAINER 304)
S165
308
USAGE LOG DATA
Kc, 199, 196, CF
COMMUNICATION MODULE
EXTERNAL MEMORY
201
308
164
163
DECRYPTION/DECOMPRESSION MODULE
220
225
MUTUAL AUTHENTICATOR
SEMI-DISCLOSURE PROCESSOR
221
199
224
DECRYPTOR (KSES)
DECOMPRESSION UNIT
ELECTRONIC WATERMARK INFORMATION PROCESSOR
C
Kc, C
C
222
223
DECRYPTOR (Kc)
196
C
169
REPRODUCTION MODULE

FIG.64

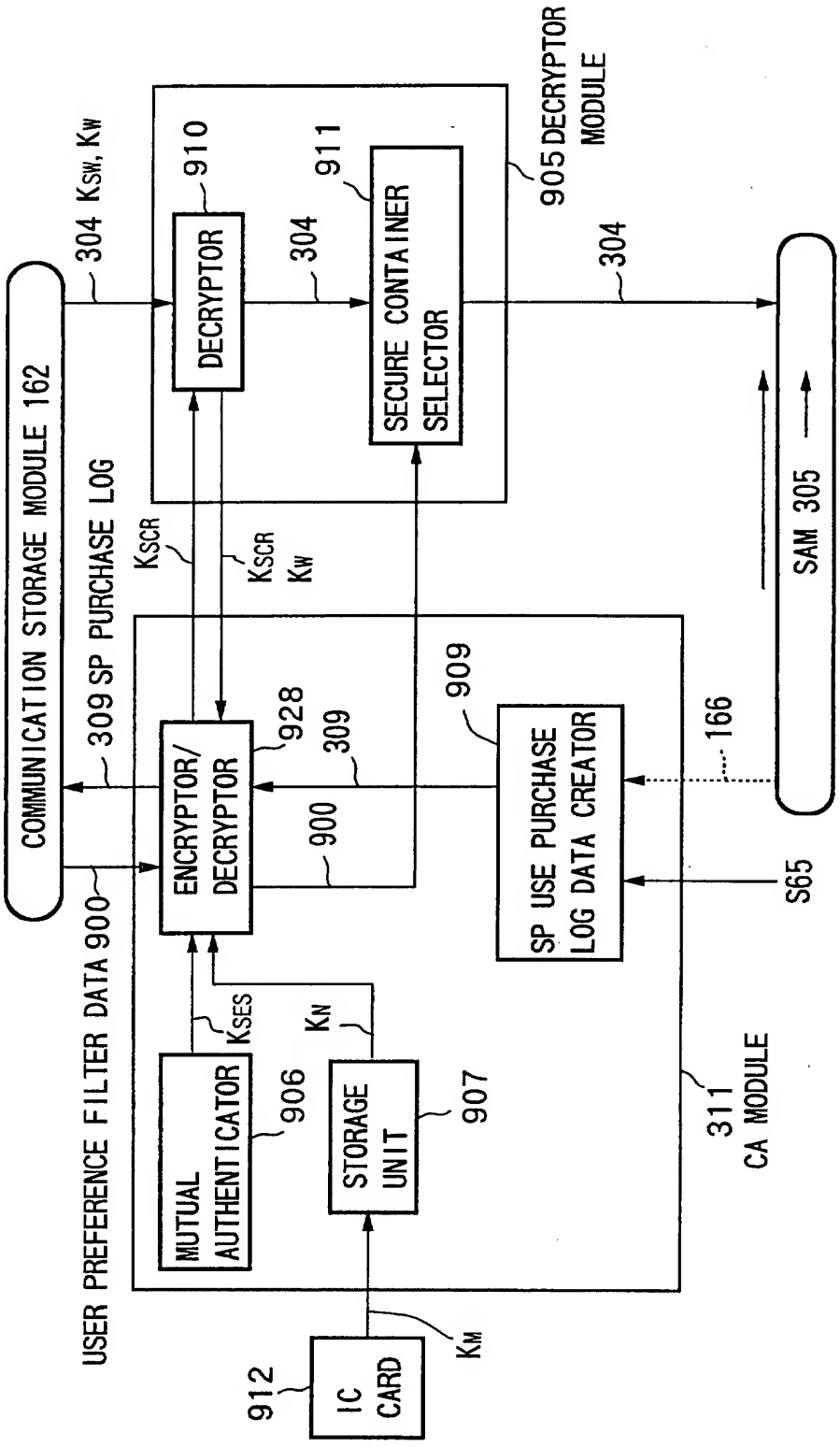

COMMUNICATION STORAGE MODULE 162
304 KSW, KW
905 DECRYPTOR MODULE
DECRYPTOR
910
911
SECURE CONTAINER SELECTOR
304
304
SAM 305
KSCR
KSCR KW
309 SP PURCHASE LOG
928
309
909
166
ENCRYPTOR/ DECRYPTOR
900
SP USE PURCHASE LOG DATA CREATOR
S65
USER PREFERENCE FILTER DATA 900
KSES
KN
MUTUAL AUTHENTICATOR
906
STORAGE UNIT
907
311 CA MODULE
912
IC CARD
KM

FIG.65

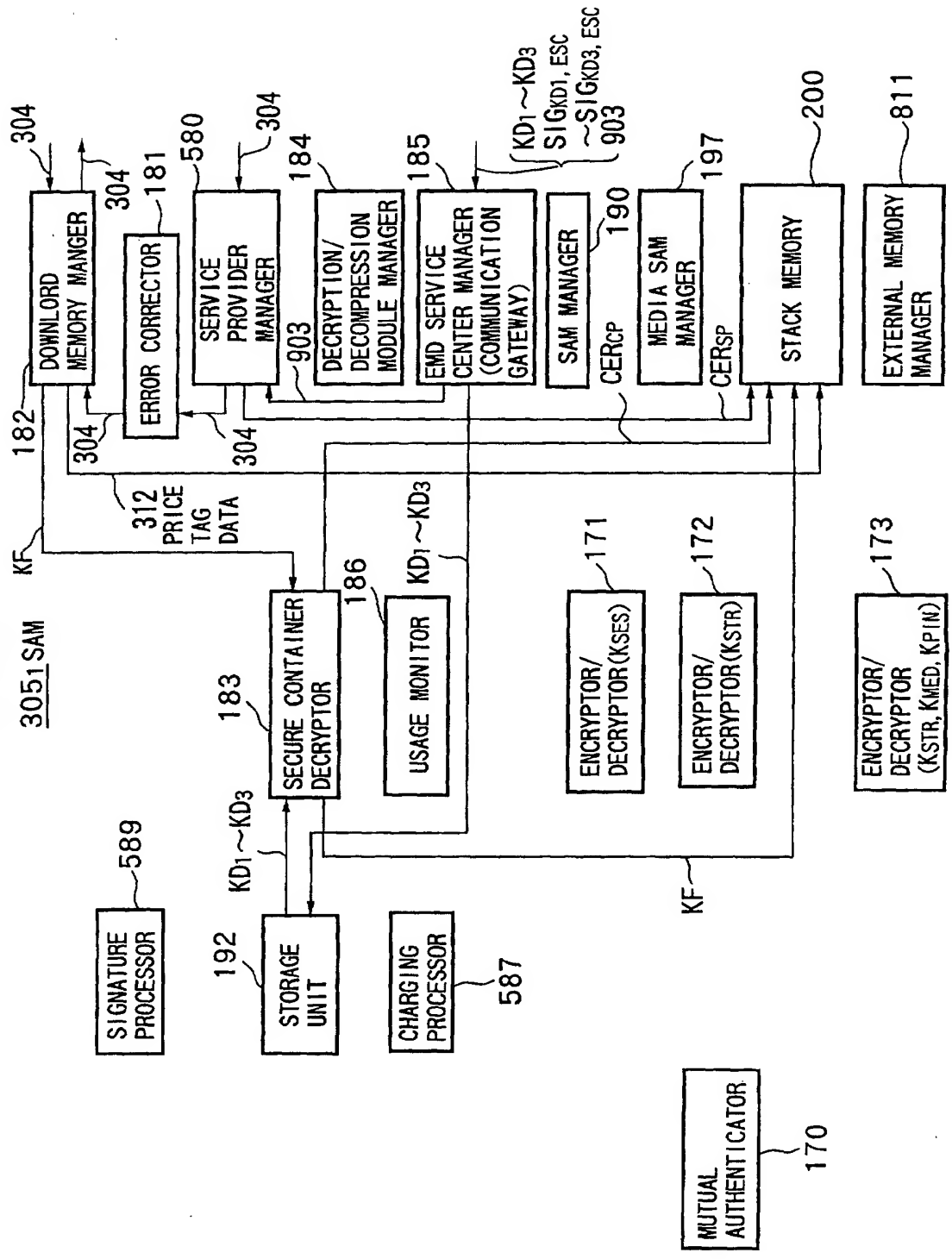

3051 SAM
DOWNLORD MEMORY MANGER
ERROR CORRECTOR
SERVICE PROVIDER MANAGER
DECRYPTION/ DECOMPRESSION MODULE MANAGER
EMD SERVICE CENTER MANAGER (COMMUNICATION GATEWAY)
SAM MANAGER
MEDIA SAM MANAGER
STACK MEMORY
EXTERNAL MEMORY MANAGER
SECURE CONTAINER DECRYPTOR
USAGE MONITOR
ENCRYPTOR/ DECRYPTOR(KSES)
ENCRYPTOR/ DECRYPTOR(KSTR)
ENCRYPTOR/ DECRYPTOR (KSTR, KMED, KPIN)
SIGNATURE PROCESSOR
STORAGE UNIT
CHARGING PROCESSOR
MUTUAL AUTHENTICATOR
312 PRICE TAG DATA
KF
KD1~KD3
SIGKD1, ESC
~SIGKD3, ESC
CERCP
CERSP
304
903
580
181
182
183
184
185
186
190
192
197
200
170
171
172
173
587
589
811

FIG.66

STORAGE DATA OF STACK MEMORY 200

CONTENT KEY DATA Kc
USAGE CONTROL POLICY DATA(UCP) 106
LOCK KEY DATA K_{LOC} OF NOVOLATILE MEMORY 201
PUBLIC KEY CERTIFICATE DATA CER_{CP} OF CONTENT PROVIDER 301
PUBLIC KEY CERTIFICATE DATA CER_{SP} OF SERVICE PROVIDER 301
USAGE CONTROL STATUS DATA(UCS) 166
SAM PROGRAM DOWNLOAD CONTAINER SD_1 TO SDC_3
PRICE TAG DATA 312

FIG.67

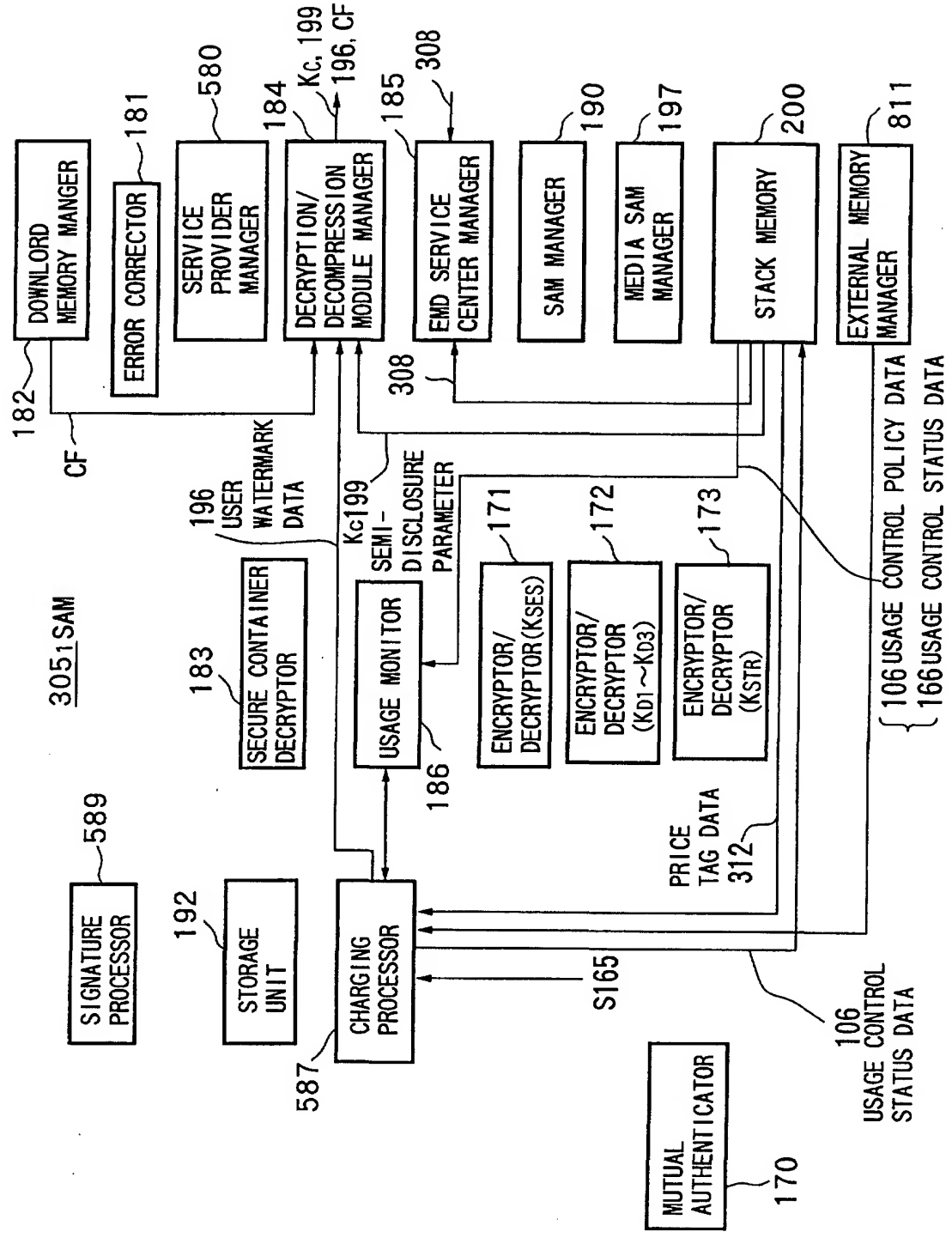
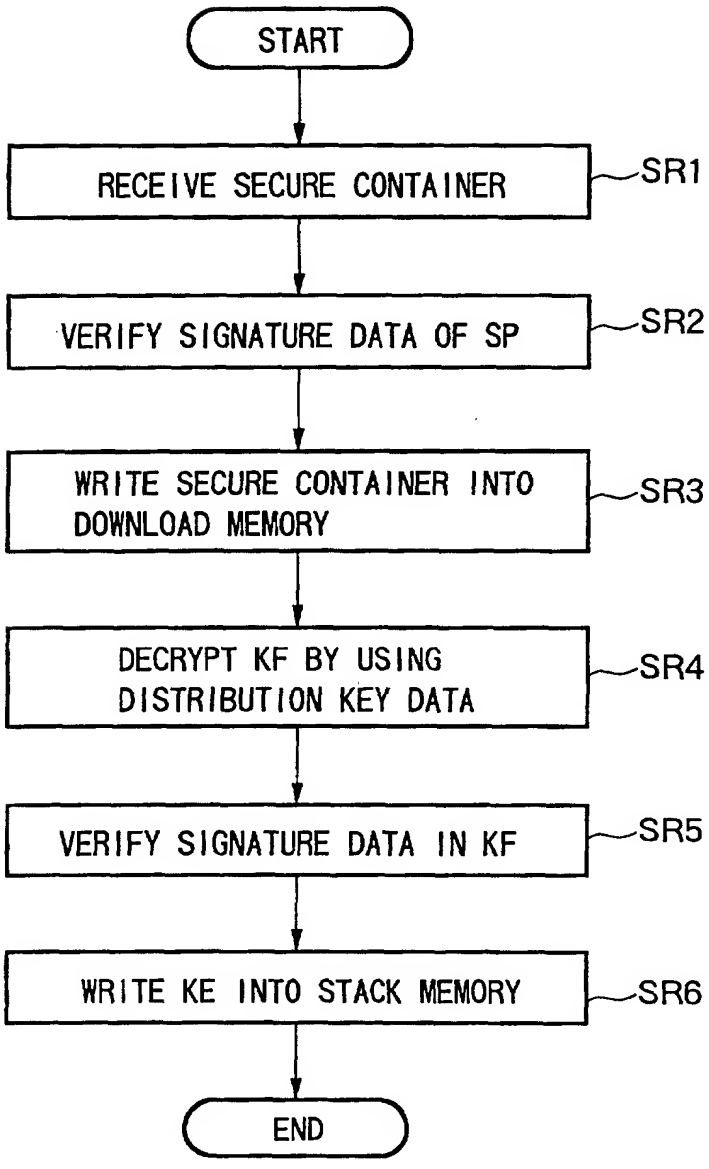
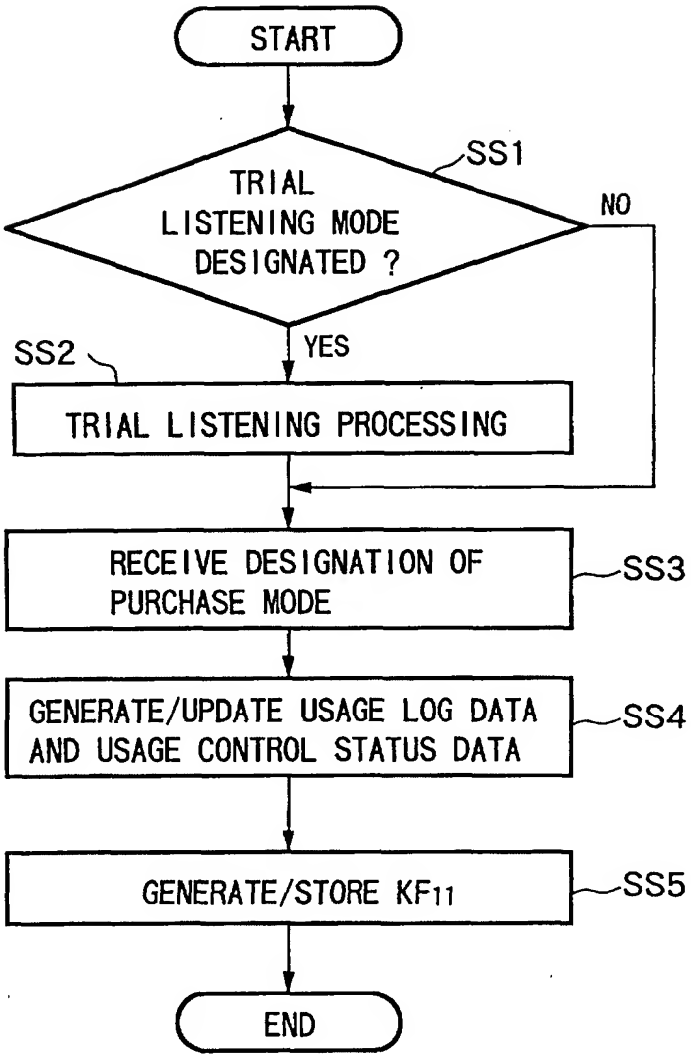

DOWNLORD MEMORY MANGER
182
CF
ERROR CORRECTOR
181
SERVICE PROVIDER MANAGER
580
DECRYPTION/ DECOMPRESSION MODULE MANAGER
184
185
Kc, 199
196, CF
EMD SERVICE CENTER MANAGER
308
SAM MANAGER
190
MEDIA SAM MANAGER
197
STACK MEMORY
200
EXTERNAL MEMORY MANAGER
811
106 USAGE CONTROL POLICY DATA
166 USAGE CONTROL STATUS DATA
196 USER WATERMARK DATA
Kc199
SEMI-DISCLOSURE PARAMETER
308
3051 SAM
183
SECURE CONTAINER DECRYPTOR
USAGE MONITOR
186
171
ENCRYPTOR/ DECRYPTOR(KSES)
172
ENCRYPTOR/ DECRYPTOR (KD1~KD3)
173
ENCRYPTOR/ DECRYPTOR (KSTR)
PRICE TAG DATA
312
589
SIGNATURE PROCESSOR
192
STORAGE UNIT
587
CHARGING PROCESSOR
S165
106 USAGE CONTROL STATUS DATA
MUTUAL AUTHENTICATOR
170

FIG.68



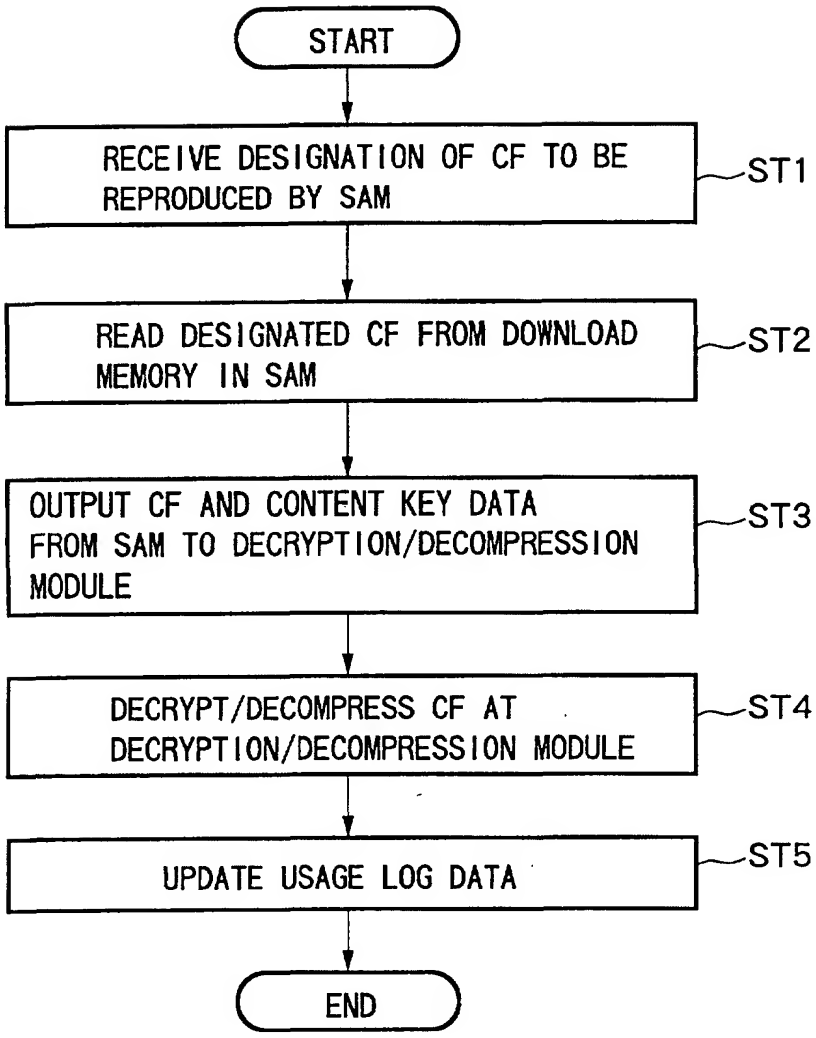
PROCESSING FOR DECRYPTION OF KF IN SAM

FIG.69



PROCESSING FOR DETERMINATION OF PURCHASE MODE OF SECURE CONTAINER IN SAM

FIG.70



PROCESSING FOR REPRODUCTION OF CONTENT DATA

FIG.71

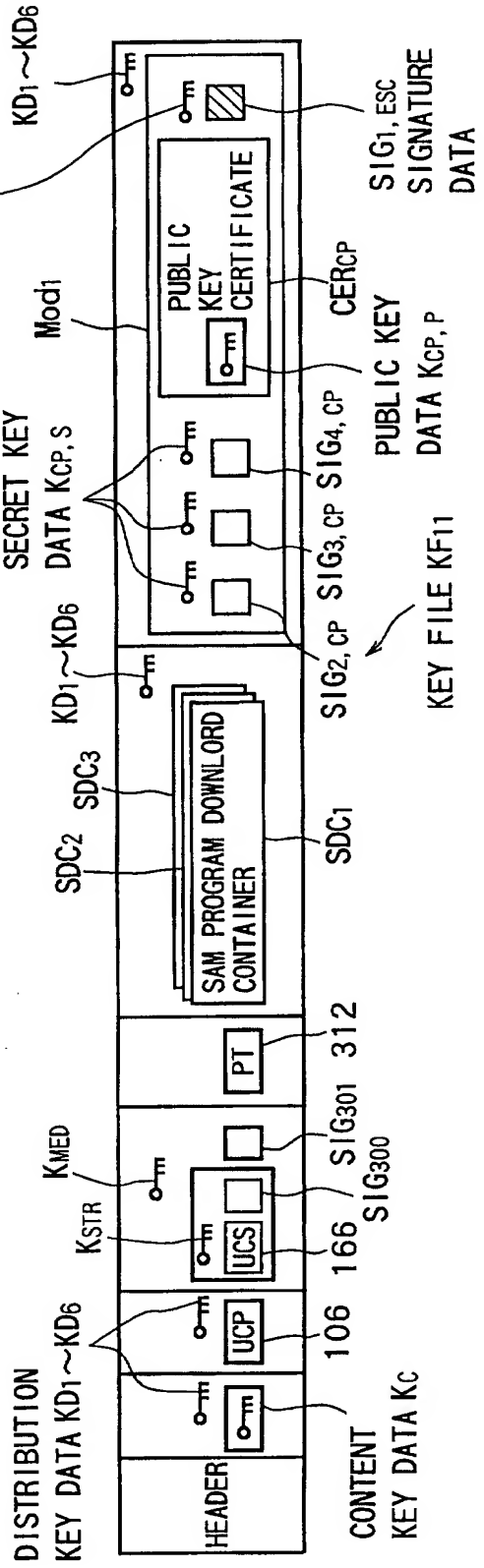

DISTRIBUTION KEY DATA KD1~KD6
HEADER
UCP
106
UCS
166
KSTR
KMED
SIG300
SIG301
PT
312
SAM PROGRAM DOWNLORD CONTAINER
SDC1
SDC2
SDC3
KD1~KD6
SECRET KEY DATA KCP, S
Mod1
SIG2, CP
SIG3, CP
SIG4, CP
PUBLIC KEY CERTIFICATE
CERCP
SECRET KEY DATA KESC, S
KD1~KD6
SIG1, ESC
CONTENT KEY DATA KC
KEY FILE KF11
PUBLIC KEY DATA KCP, P
SIGNATURE DATA

FIG.72

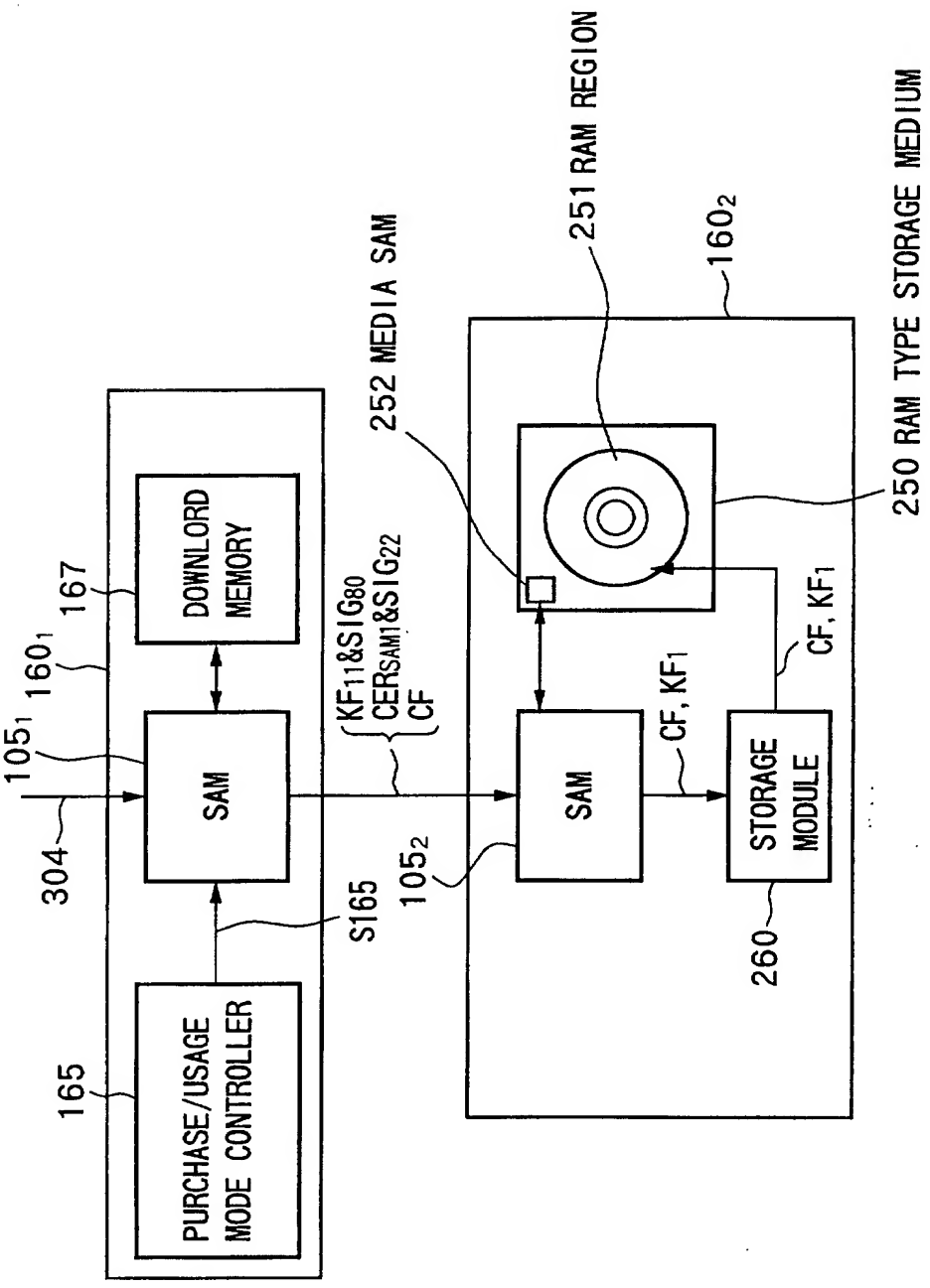

250 RAM TYPE STORAGE MEDIUM
251 RAM REGION
252 MEDIA SAM
160_2
160_1
167
DOWNLORD MEMORY
105_1
SAM
304
165
PURCHASE/USAGE MODE CONTROLLER
S165
KF_{11}&SIG_{80}
CER_{SAM1}&SIG_{22}
CF
105_2
SAM
CF, KF_1
STORAGE MODULE
260
CF, KF_1

FIG.73

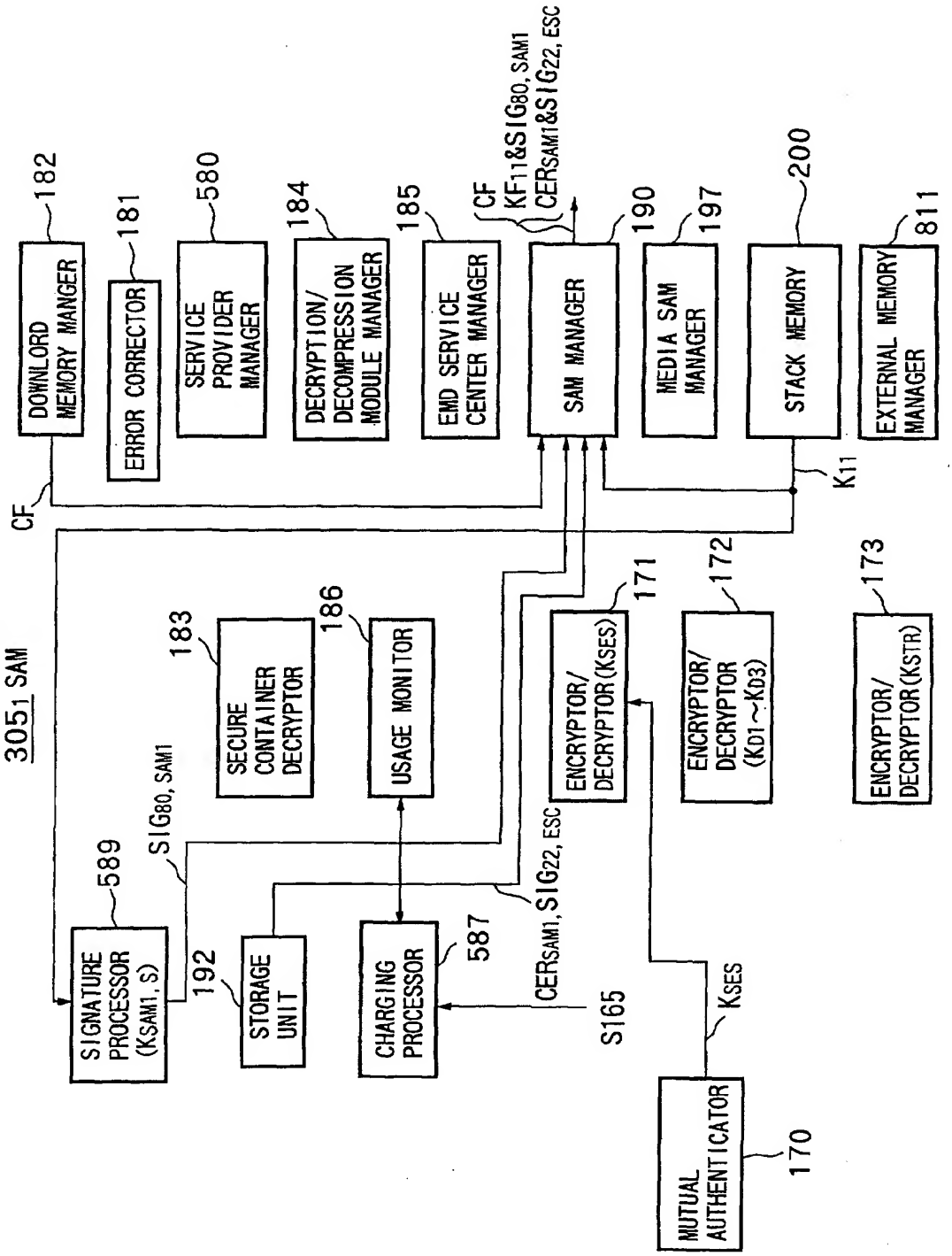
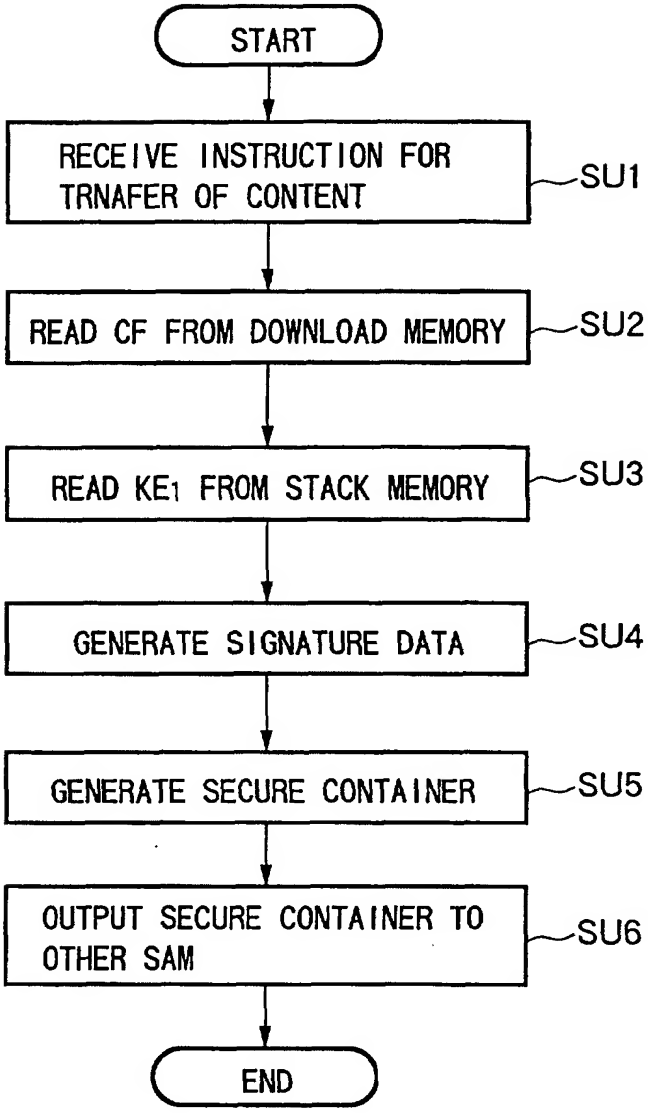

3051 SAM
DOWNLORD MEMORY MANGER
182
ERROR CORRECTOR
181
SERVICE PROVIDER MANAGER
580
DECRYPTION/ DECOMPRESSION MODULE MANAGER
184
EMD SERVICE CENTER MANAGER
185
CF
KF11&SIG80, SAM1
CERSAM1&SIG22, ESC
SAM MANAGER
190
MEDIA SAM MANAGER
197
STACK MEMORY
200
EXTERNAL MEMORY MANAGER
811
CF
K11
SECURE CONTAINER DECRYPTOR
183
USAGE MONITOR
186
ENCRYPTOR/ DECRYPTOR(KSES)
171
ENCRYPTOR/ DECRYPTOR (KD1~KD3)
172
ENCRYPTOR/ DECRYPTOR(KSTR)
173
SIG80, SAM1
SIG22, ESC
CERSAM1,
589
SIGNATURE PROCESSOR (KSAM1, S)
192
STORAGE UNIT
CHARGING PROCESSOR
587
S165
KSES
MUTUAL AUTHENTICATOR
170

FIG.74



PROCESSING OF SAM FOR TRANSFERRING CONTENT AFTER DETERMINING PURCHASE MODE TO OTHER SAM

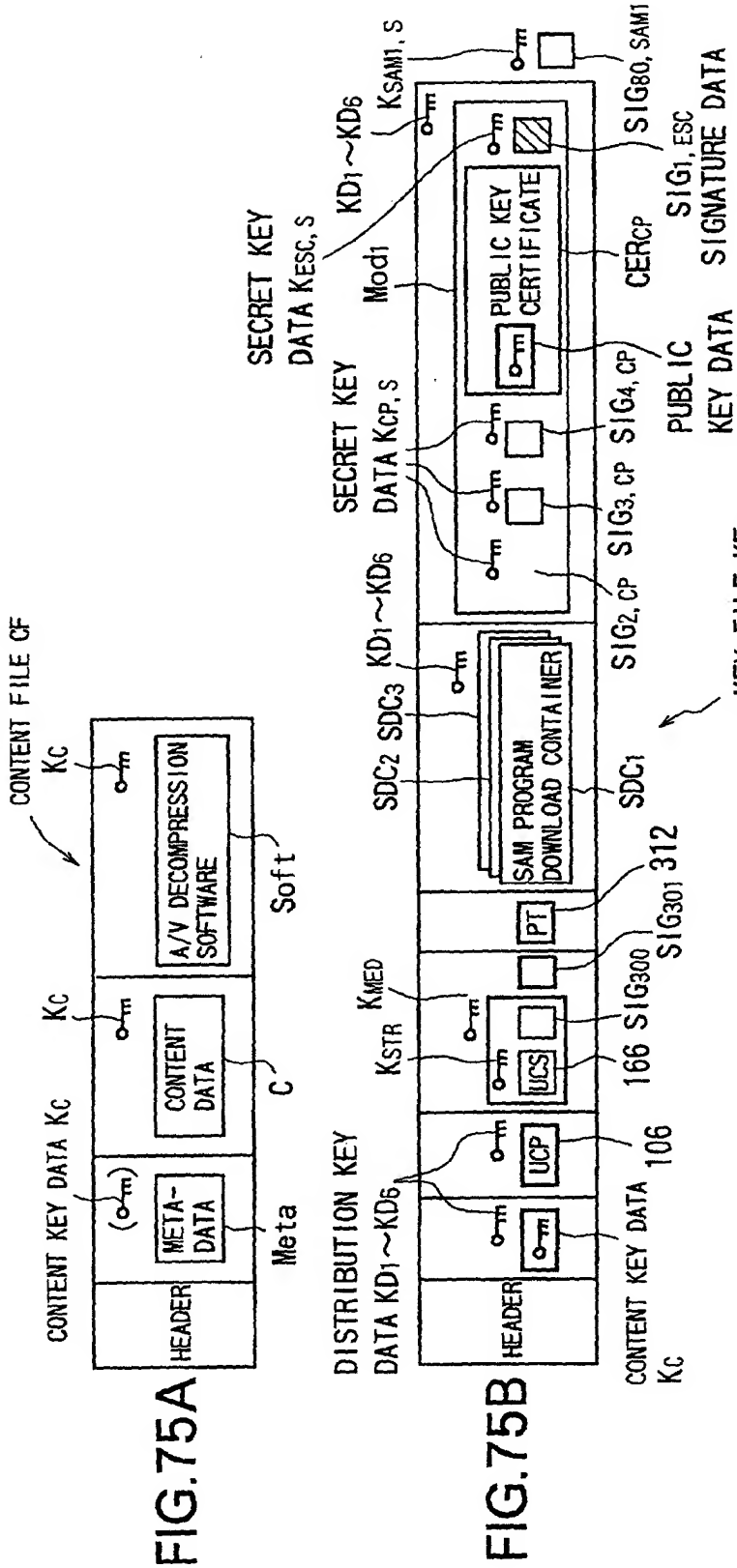

CONTENT FILE CF
Kc
CONTENT KEY DATA Kc
HEADER
META-DATA
Meta
CONTENT DATA
C
A/V DECOMPRESSION SOFTWARE
Soft
FIG.75A
SECRET KEY DATA KESC, S
KD1~KD6
KSAM1, S
SECRET KEY DATA KCP, S
Mod1
PUBLIC KEY CERTIFICATE
CERCP
SIG1, ESC
SIG80, SAM1
SIG2, CP
SIG3, CP
SIG4, CP
PUBLIC KEY DATA KCP, P
SIGNATURE DATA
KEY FILE KF11
SDC2 SDC3
SDC1
SAM PROGRAM DOWNLOAD CONTAINER
PT
312
SIG301
KMED
KSTR
UCS
166
SIG300
UCP
106
DISTRIBUTION KEY DATA KD1~KD6
HEADER
CONTENT KEY DATA Kc
FIG.75B
KESC, S
SIG22, ESC
PUBLIC KEY CERTIFICATE
KSAM1, P
CERSAM1
FIG.75C

FIG.76

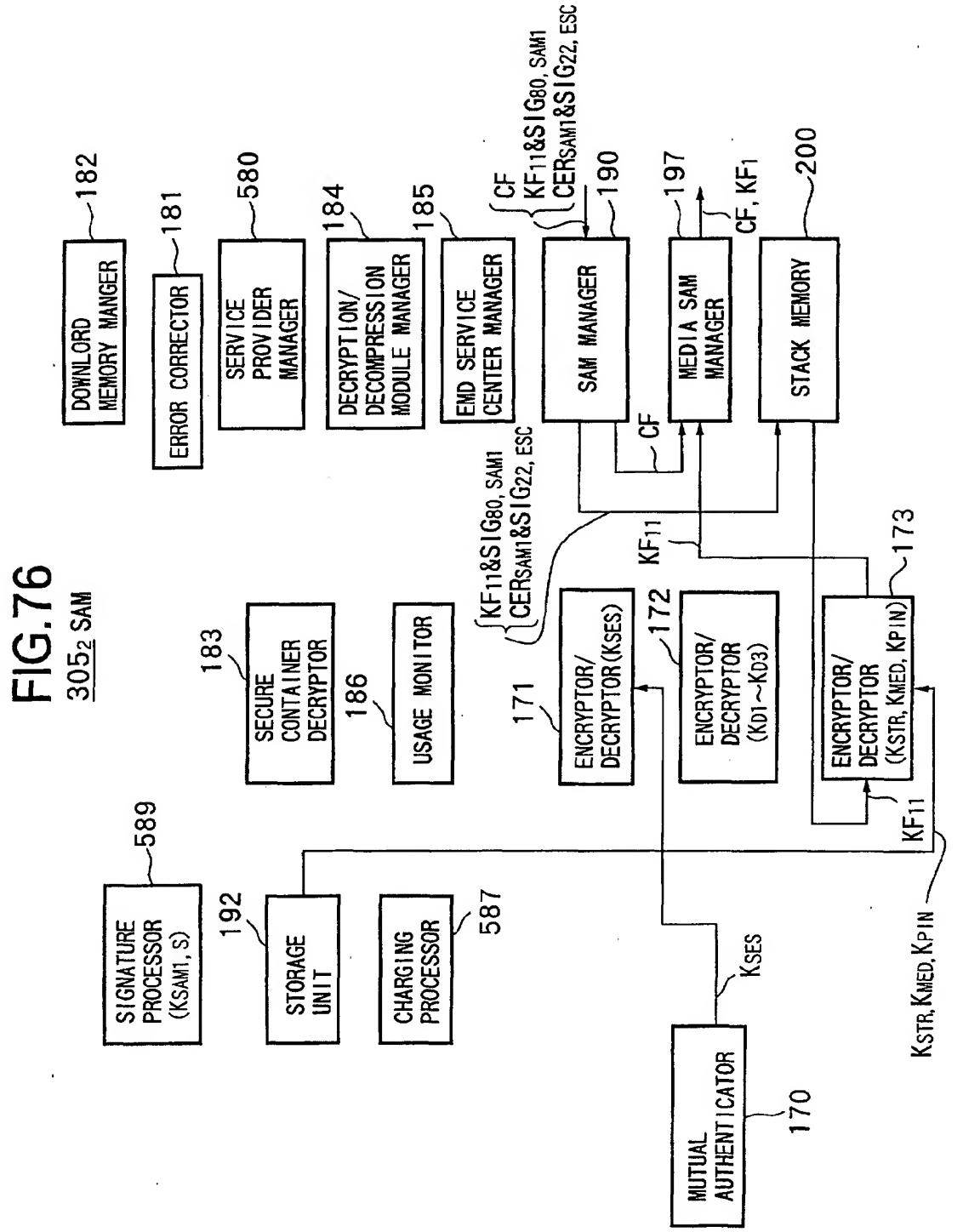
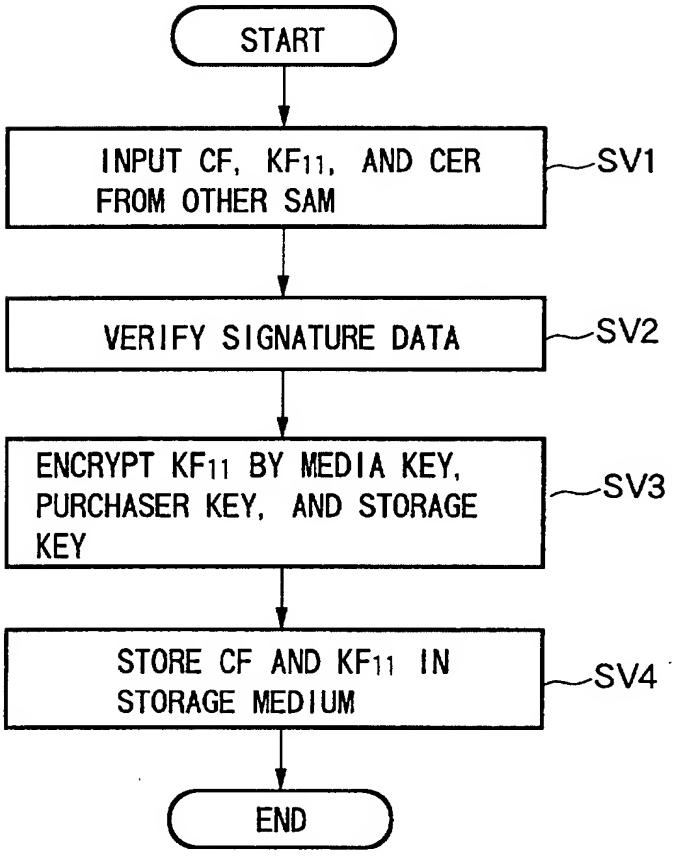

305_2 SAM
182
DOWNLORD MEMORY MANGER
181
ERROR CORRECTOR
580
SERVICE PROVIDER MANAGER
184
DECRYPTION/ DECOMPRESSION MODULE MANAGER
185
EMD SERVICE CENTER MANAGER
CF
KF11&SIG80, SAM1
CERSAM1&SIG22, ESC
190
SAM MANAGER
197
MEDIA SAM MANAGER
CF, KF1
200
STACK MEMORY
CF
KF11&SIG80, SAM1
CERSAM1&SIG22, ESC
KF11
173
183
SECURE CONTAINER DECRYPTOR
186
USAGE MONITOR
171
ENCRYPTOR/ DECRYPTOR(KSES)
172
ENCRYPTOR/ DECRYPTOR (KD1~KD3)
ENCRYPTOR/ DECRYPTOR (KSTR, KMED, KPIN)
589
SIGNATURE PROCESSOR (KSAM1, S)
192
STORAGE UNIT
587
CHARGING PROCESSOR
KF11
KSES
MUTUAL AUTHENTICATOR
170
KSTR, KMED, KPIN

FIG.77



PROCESSING OF SAM WHEN WRITING CF, ETC. INPUT FROM OTHER SAM INTO STORAGE MEDIUM

FIG.78

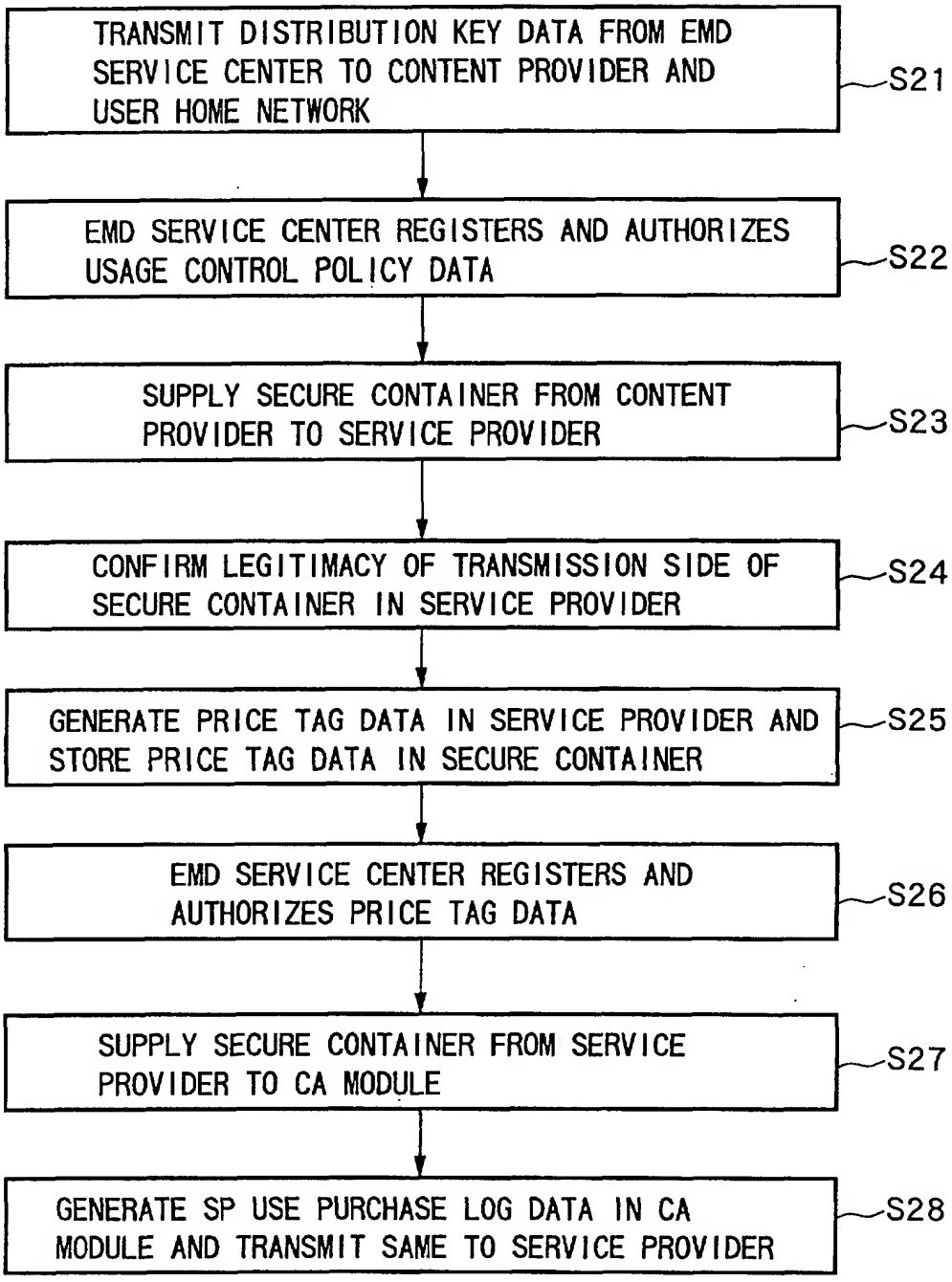

TRANSMIT DISTRIBUTION KEY DATA FROM EMD SERVICE CENTER TO CONTENT PROVIDER AND USER HOME NETWORK
S21
EMD SERVICE CENTER REGISTERS AND AUTHORIZES USAGE CONTROL POLICY DATA
S22
SUPPLY SECURE CONTAINER FROM CONTENT PROVIDER TO SERVICE PROVIDER
S23
CONFIRM LEGITIMACY OF TRANSMISSION SIDE OF SECURE CONTAINER IN SERVICE PROVIDER
S24
GENERATE PRICE TAG DATA IN SERVICE PROVIDER AND STORE PRICE TAG DATA IN SECURE CONTAINER
S25
EMD SERVICE CENTER REGISTERS AND AUTHORIZES PRICE TAG DATA
S26
SUPPLY SECURE CONTAINER FROM SERVICE PROVIDER TO CA MODULE
S27
GENERATE SP USE PURCHASE LOG DATA IN CA MODULE AND TRANSMIT SAME TO SERVICE PROVIDER
S28

FIG.79

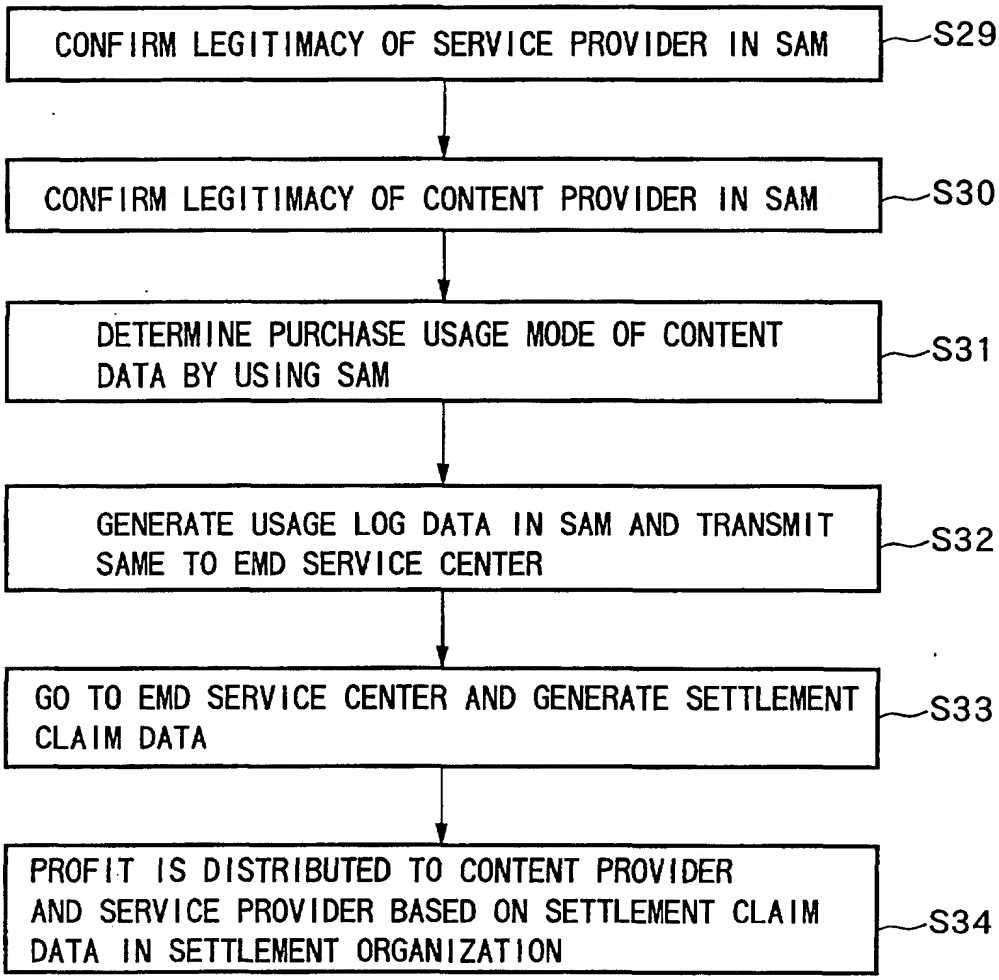

CONFIRM LEGITIMACY OF SERVICE PROVIDER IN SAM
S29
CONFIRM LEGITIMACY OF CONTENT PROVIDER IN SAM
S30
DETERMINE PURCHASE USAGE MODE OF CONTENT DATA BY USING SAM
S31
GENERATE USAGE LOG DATA IN SAM AND TRANSMIT SAME TO EMD SERVICE CENTER
S32
GO TO EMD SERVICE CENTER AND GENERATE SETTLEMENT CLAIM DATA
S33
PROFIT IS DISTRIBUTED TO CONTENT PROVIDER AND SERVICE PROVIDER BASED ON SETTLEMENT CLAIM DATA IN SETTLEMENT ORGANIZATION
S34

FIG.80

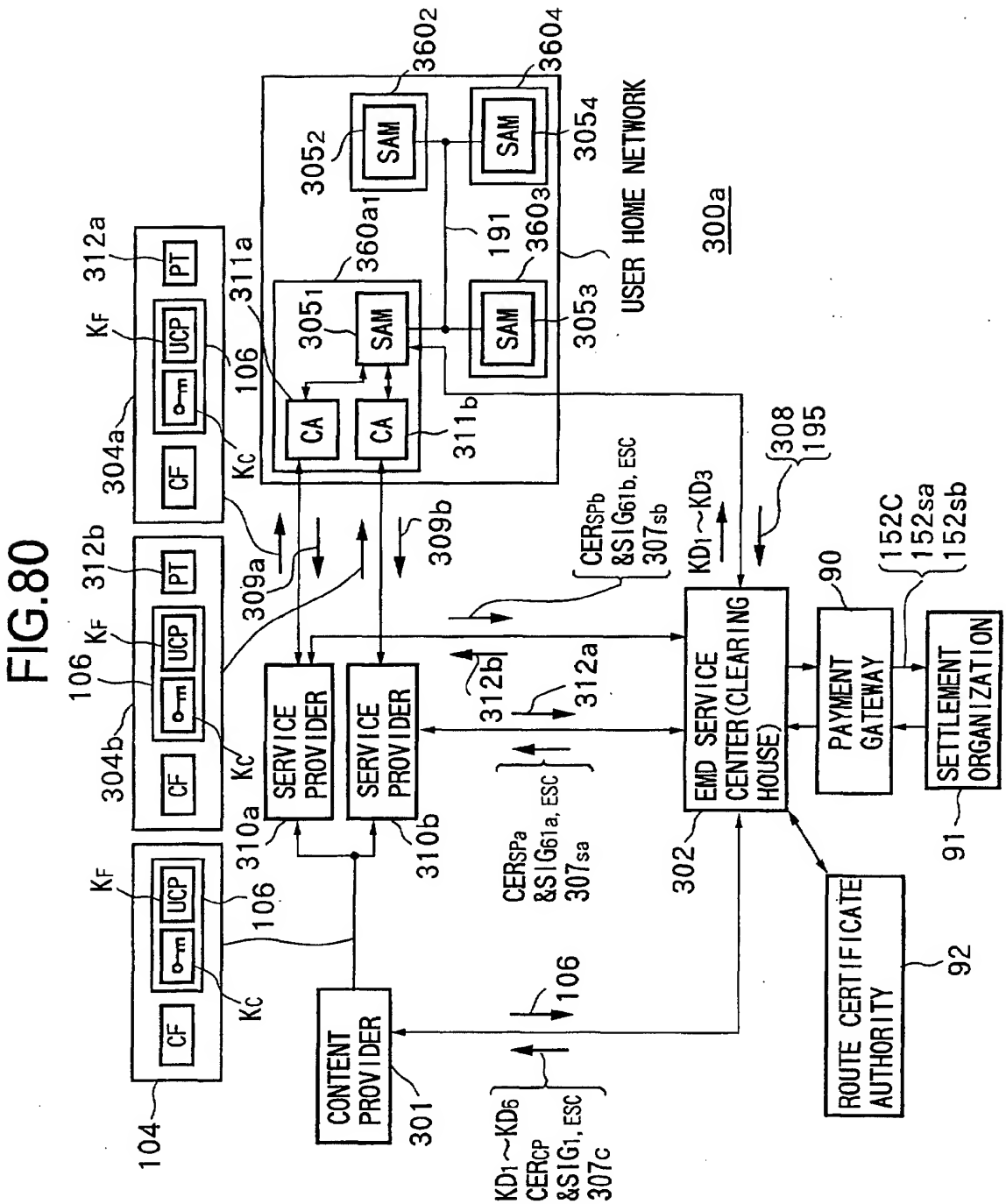

USER HOME NETWORK
300a
CONTENT PROVIDER
301
SERVICE PROVIDER
SERVICE PROVIDER
EMD SERVICE CENTER(CLEARING HOUSE)
302
PAYMENT GATEWAY
SETTLEMENT ORGANIZATION
ROUTE CERTIFICATE AUTHORITY
CA
CA
SAM
SAM
SAM
SAM
CF
UCP
PT
106
191
195
308
90
91
92
104
152C
152sa
152sb
309a
309b
310a
310b
311a
311b
312a
312b
304a
304b
360a1
360₂
360₃
360₄
305₁
305₂
305₃
305₄
Kc
KF
KD1~KD3
KD1~KD6
CERCP &SIG1, ESC 307c
CERSPa &SIG61a, ESC 307sa
CERSPb &SIG61b, ESC 307sb

FIG.81

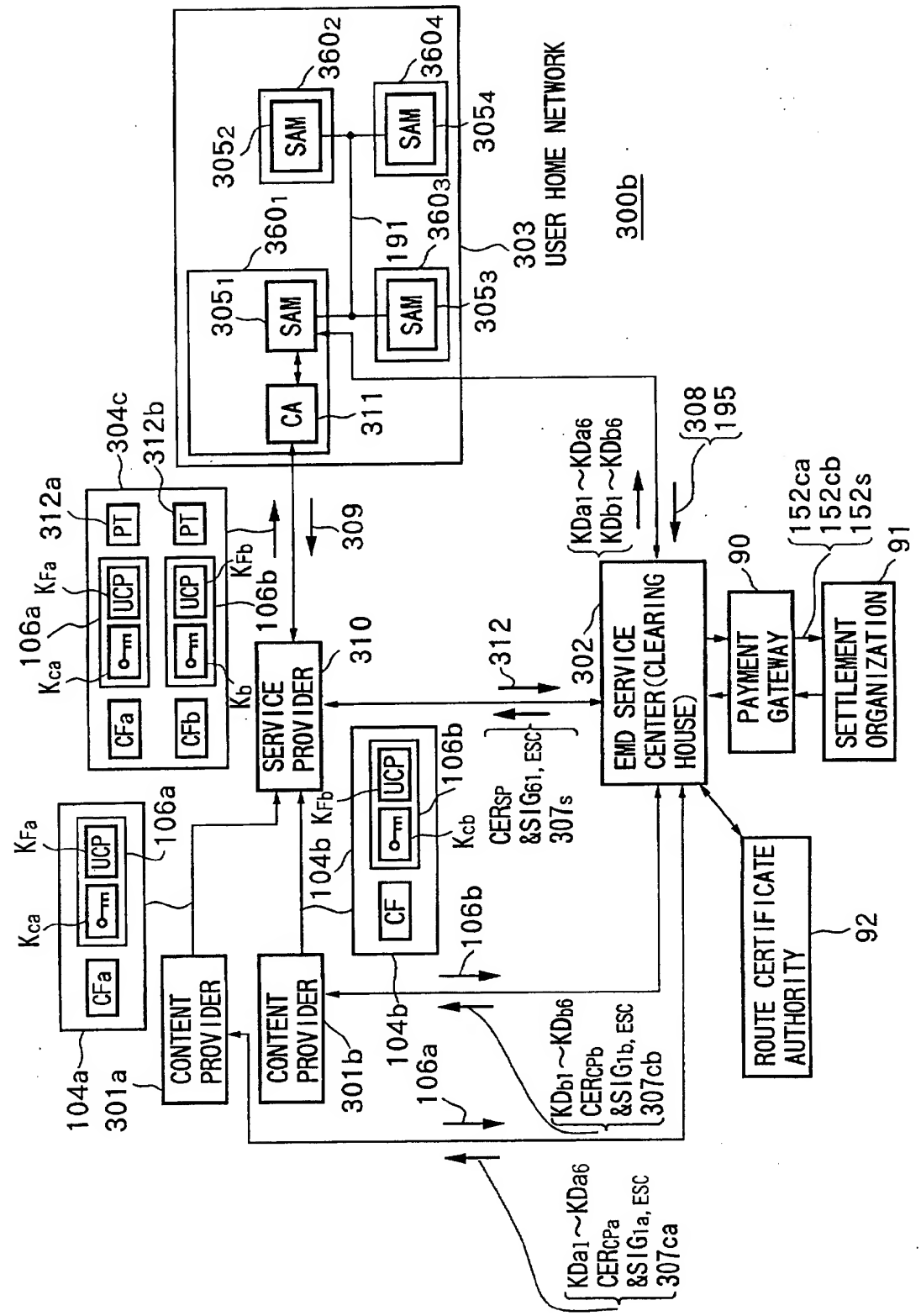

USER HOME NETWORK
300b
303
SAM
CA
SERVICE PROVIDER
CONTENT PROVIDER
CONTENT PROVIDER
EMD SERVICE CENTER(CLEARING HOUSE)
PAYMENT GATEWAY
SETTLEMENT ORGANIZATION
ROUTE CERTIFICATE AUTHORITY
CF
CFa
CFb
UCP
PT
191
195
302
308
309
310
311
312
90
91
92

FIG.82

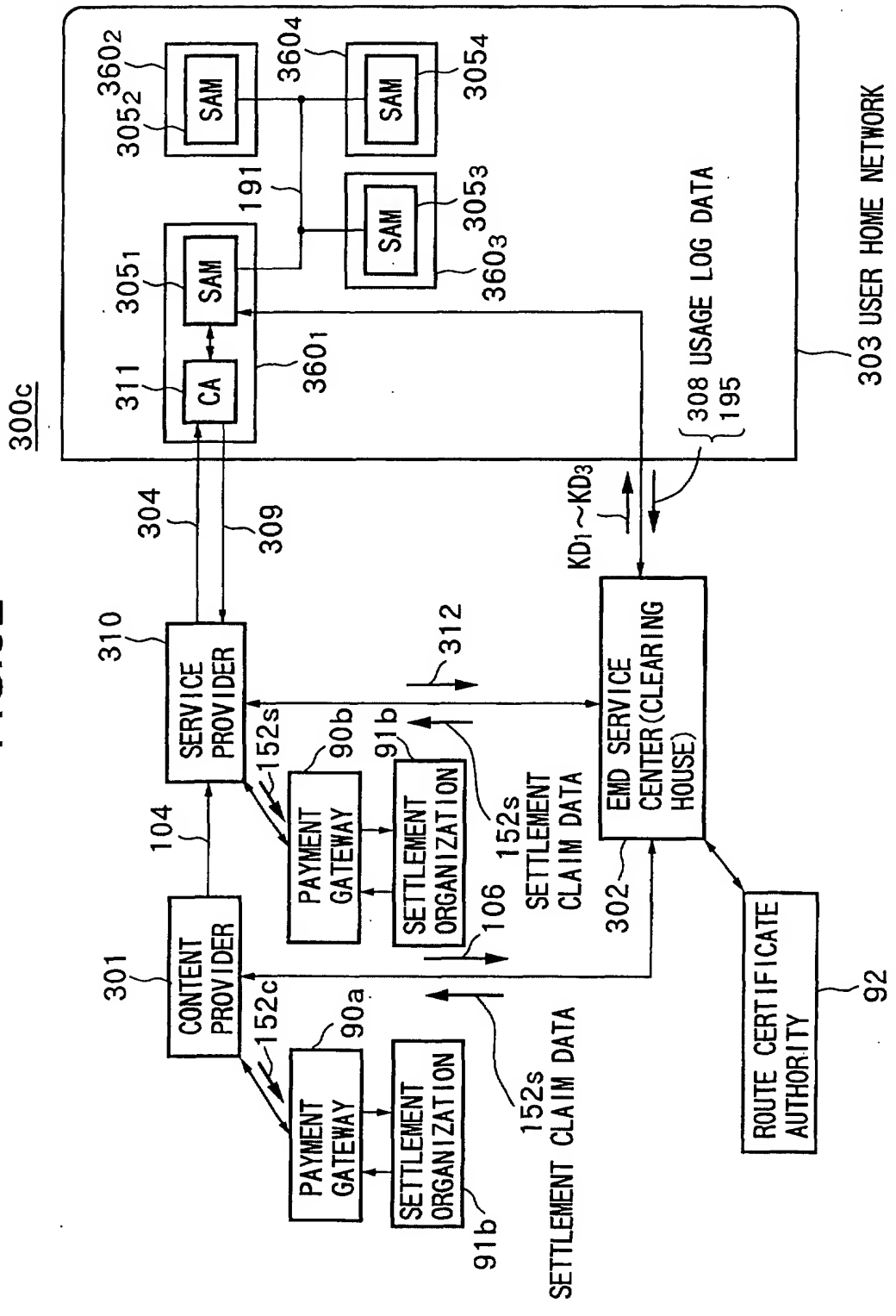

300c
303 USER HOME NETWORK
308 USAGE LOG DATA
195
SAM
CA
311
191
304
309
310
SERVICE PROVIDER
312
KD1~KD3
EMD SERVICE CENTER(CLEARING HOUSE)
302
152s SETTLEMENT CLAIM DATA
152s SETTLEMENT CLAIM DATA
PAYMENT GATEWAY
SETTLEMENT ORGANIZATION
CONTENT PROVIDER
301
104
106
152s
152c
90a
90b
91b
ROUTE CERTIFICATE AUTHORITY
92

FIG.83

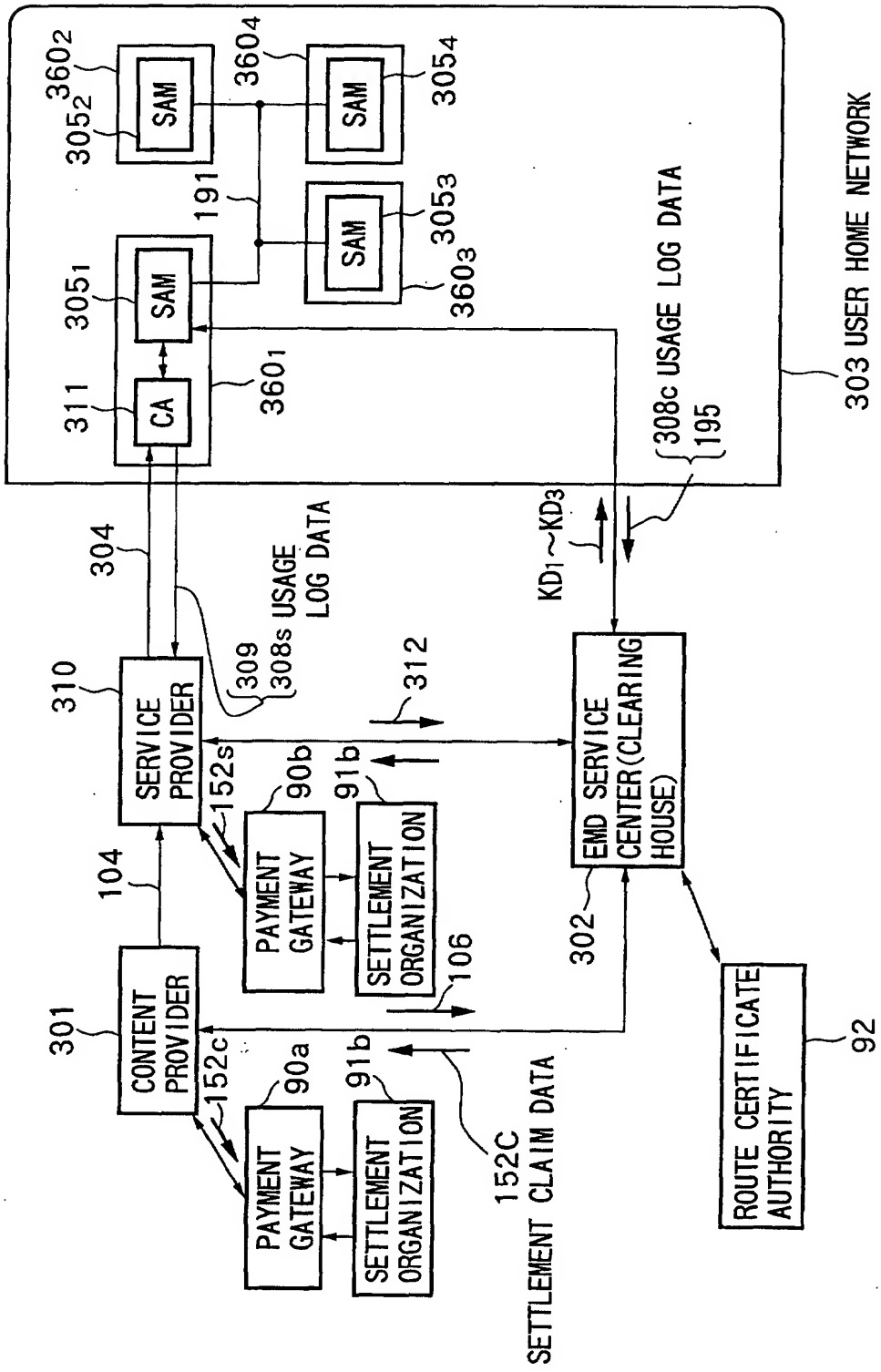

3602
3052
SAM
3604
SAM
3054
191
SAM
3053
3603
3051
SAM
3601
311
CA
303 USER HOME NETWORK
308c USAGE LOG DATA
195
304
KD1~KD3
308s USAGE LOG DATA
309
310
SERVICE PROVIDER
312
152s
90b
91b
PAYMENT GATEWAY
SETTLEMENT ORGANIZATION
EMD SERVICE CENTER(CLEARING HOUSE)
104
106
302
301
CONTENT PROVIDER
152c
90a
91b
PAYMENT GATEWAY
SETTLEMENT ORGANIZATION
152C
SETTLEMENT CLAIM DATA
ROUTE CERTIFICATE AUTHORITY
92

FIG.84

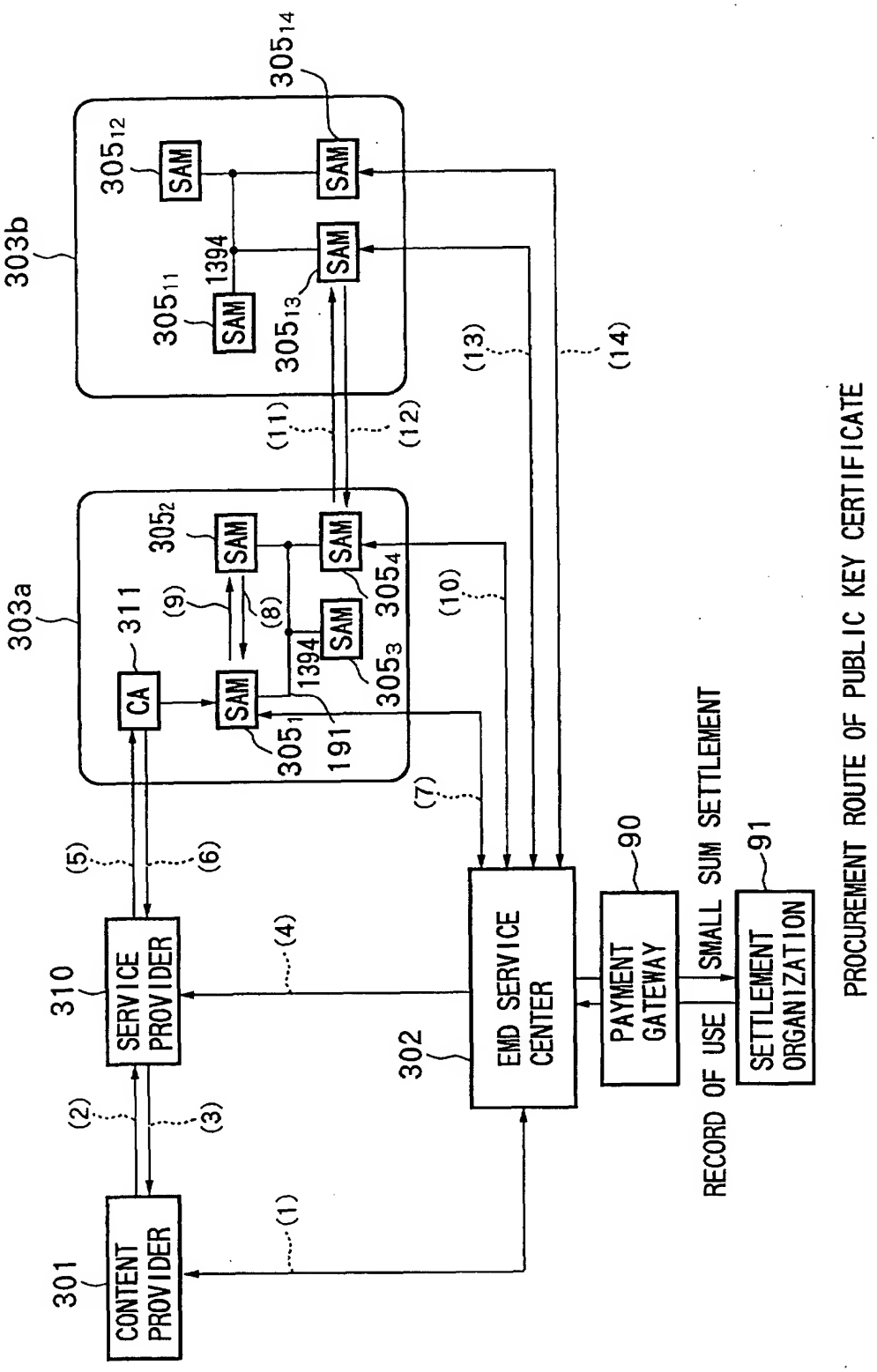

303b
303a
305_{14}
305_{12}
305_{11}
305_{13}
305_2
305_4
305_3
305_1
SAM
1394
CA
311
191
(1)
(2)
(3)
(4)
(5)
(6)
(7)
(8)
(9)
(10)
(11)
(12)
(13)
(14)
301
CONTENT PROVIDER
310
SERVICE PROVIDER
302
EMD SERVICE CENTER
90
PAYMENT GATEWAY
91
SETTLEMENT ORGANIZATION
RECORD OF USE
SMALL SUM SETTLEMENT
PROCUREMENT ROUTE OF PUBLIC KEY CERTIFICATE

FIG.85

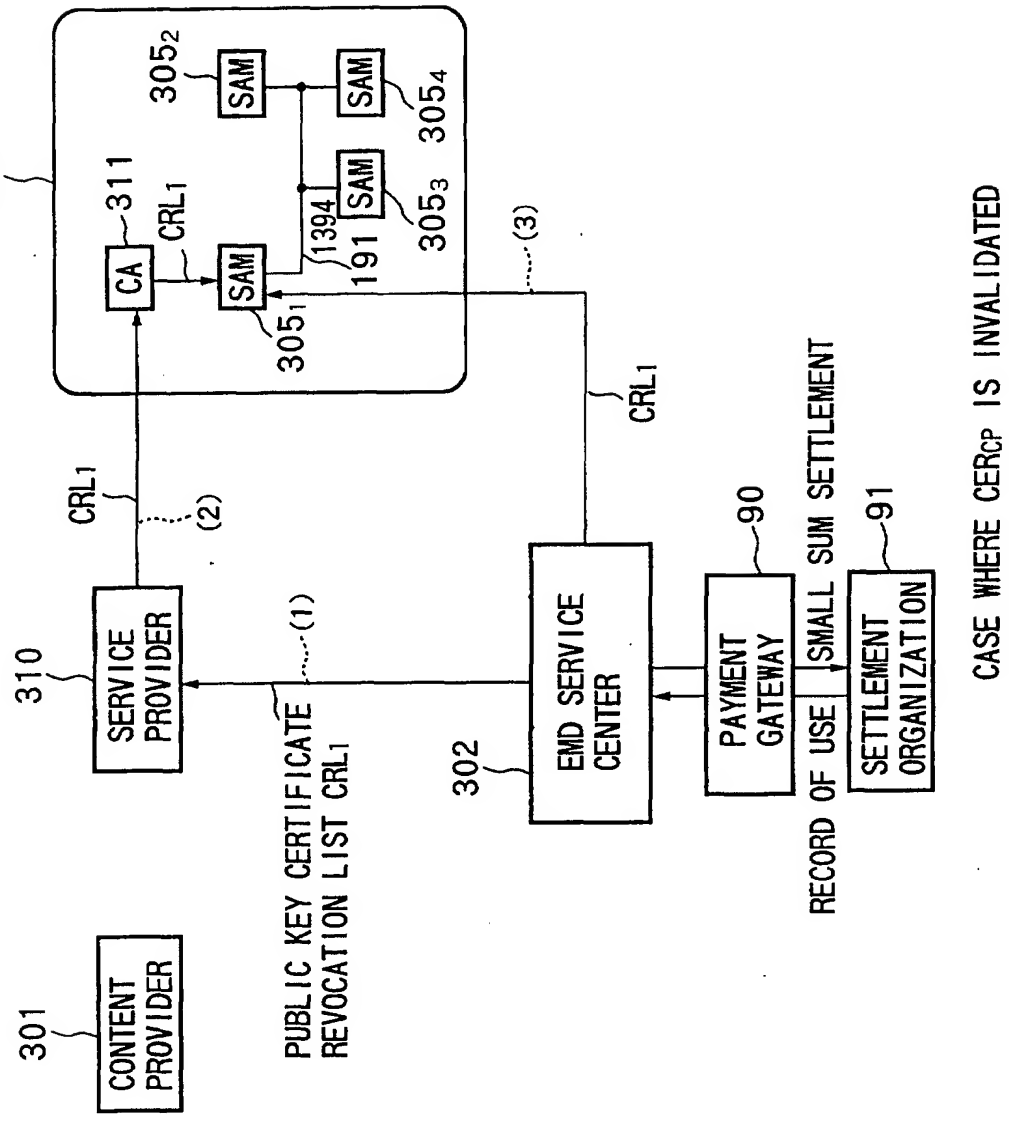

303
311
CA
CRL1
SAM
305₁
1394
191
SAM
305₃
SAM
305₂
SAM
305₄
(3)
CRL1
CRL1
(2)
310
SERVICE PROVIDER
(1)
PUBLIC KEY CERTIFICATE REVOCATION LIST CRL1
302
EMD SERVICE CENTER
90
PAYMENT GATEWAY
SMALL SUM SETTLEMENT
RECORD OF USE
91
SETTLEMENT ORGANIZATION
CASE WHERE CERCP IS INVALIDATED
301
CONTENT PROVIDER

FIG.86

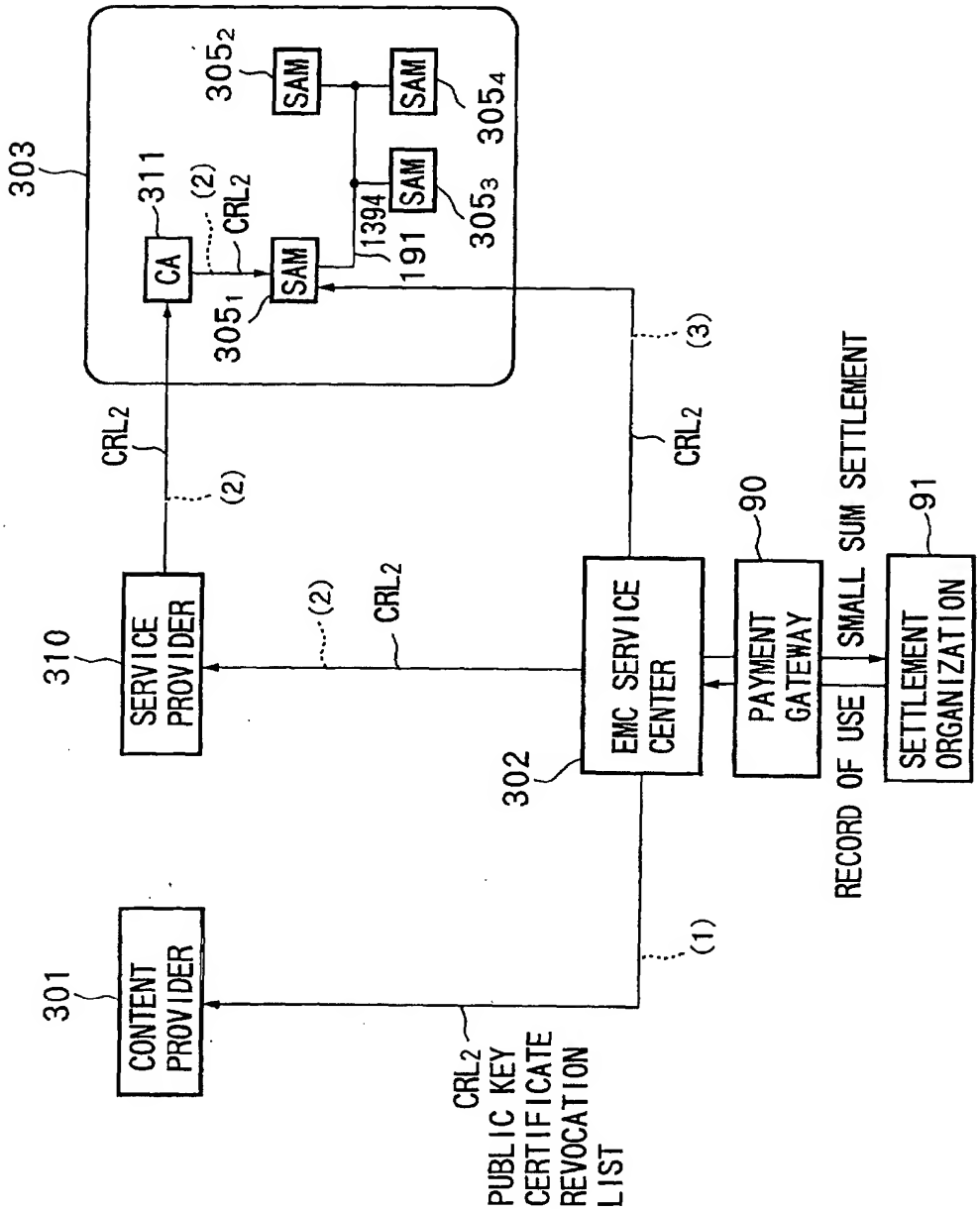

303
311
CA
(2)
CRL2
SAM
1394
191
3051
3052
3053
3054
CRL2
(2)
310
SERVICE PROVIDER
(2)
CRL2
302
EMC SERVICE CENTER
(3)
CRL2
90
PAYMENT GATEWAY
SMALL SUM SETTLEMENT
91
SETTLEMENT ORGANIZATION
RECORD OF USE
301
CONTENT PROVIDER
(1)
CRL2
PUBLIC KEY CERTIFICATE REVOCATION LIST
CASE WHERE CERSP IS INVALIDATED

FIG.87

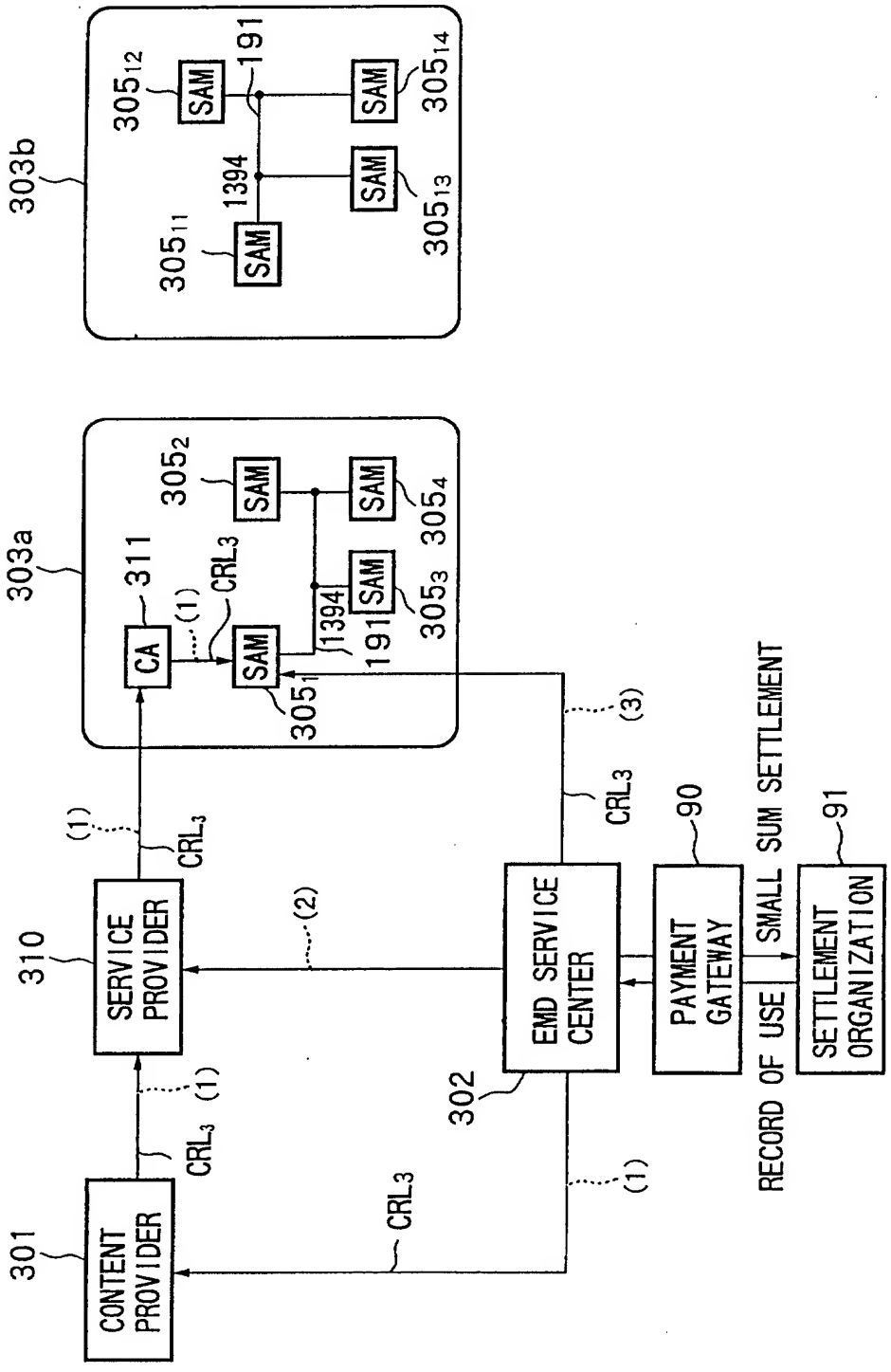

303b
305₁₂
SAM
191
SAM
305₁₄
1394
SAM
SAM
305₁₁
305₁₃
303a
311
305₂
SAM
SAM
305₄
CA
(1)
CRL₃
SAM
1394
191
SAM
305₃
305₁
(3)
CRL₃
(1)
CRL₃
310
SERVICE PROVIDER
(2)
EMD SERVICE CENTER
90
PAYMENT GATEWAY
SMALL SUM SETTLEMENT
91
SETTLEMENT ORGANIZATION
RECORD OF USE
302
(1)
CRL₃
301
CONTENT PROVIDER
CASE WHERE CERSAM2 IS INVALIDATED

FIG.88

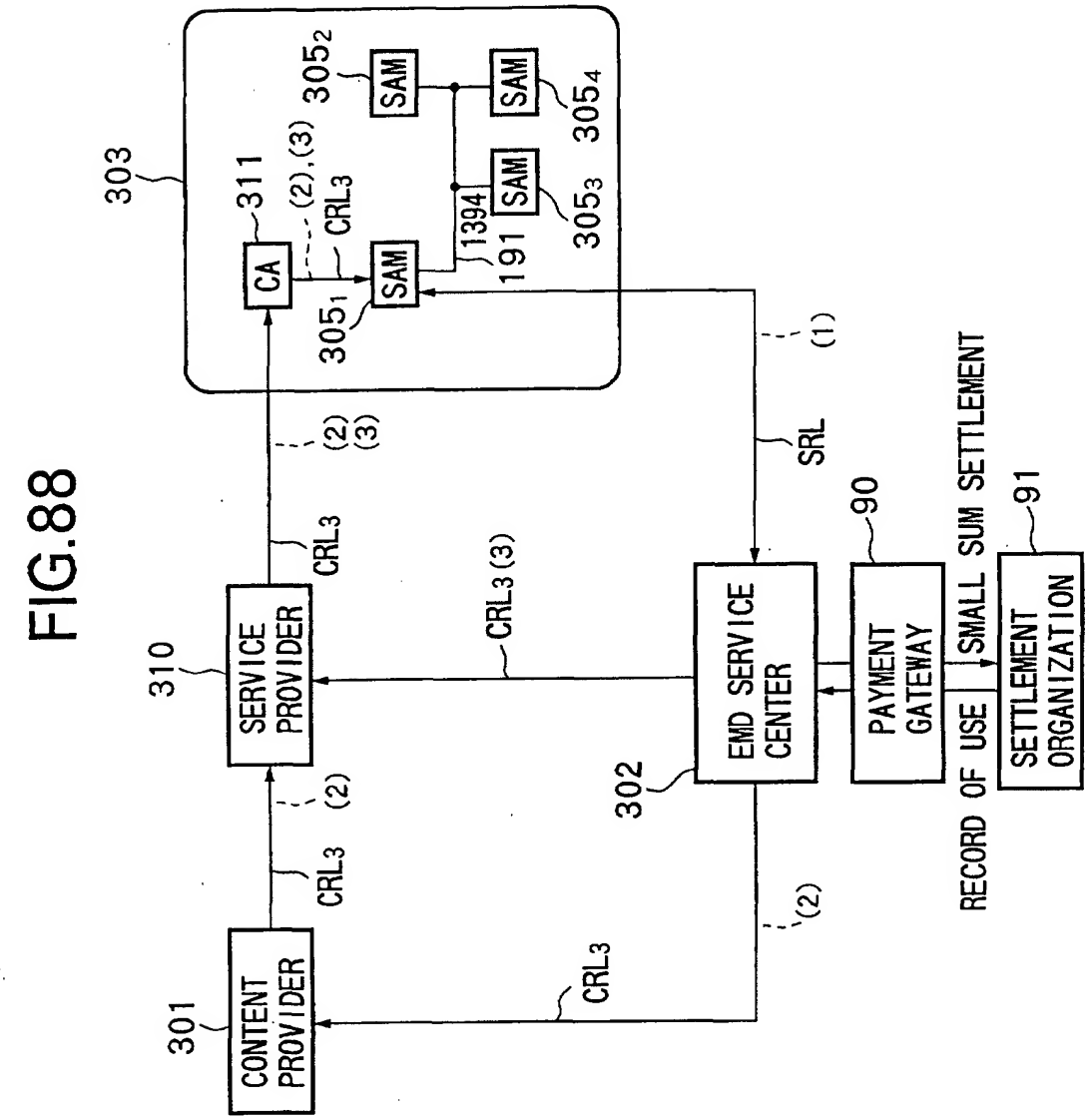

303
311
CA
(2),(3)
CRL3
SAM
3051
3052
3053
3054
1394
191
(1)
SRL
(2)
(3)
CRL3
310
SERVICE PROVIDER
CRL3 (3)
302
EMD SERVICE CENTER
90
PAYMENT GATEWAY
91
SETTLEMENT ORGANIZATION
RECORD OF USE
SMALL SUM SETTLEMENT
(2)
CRL3
301
CONTENT PROVIDER
CRL3

FIG.89

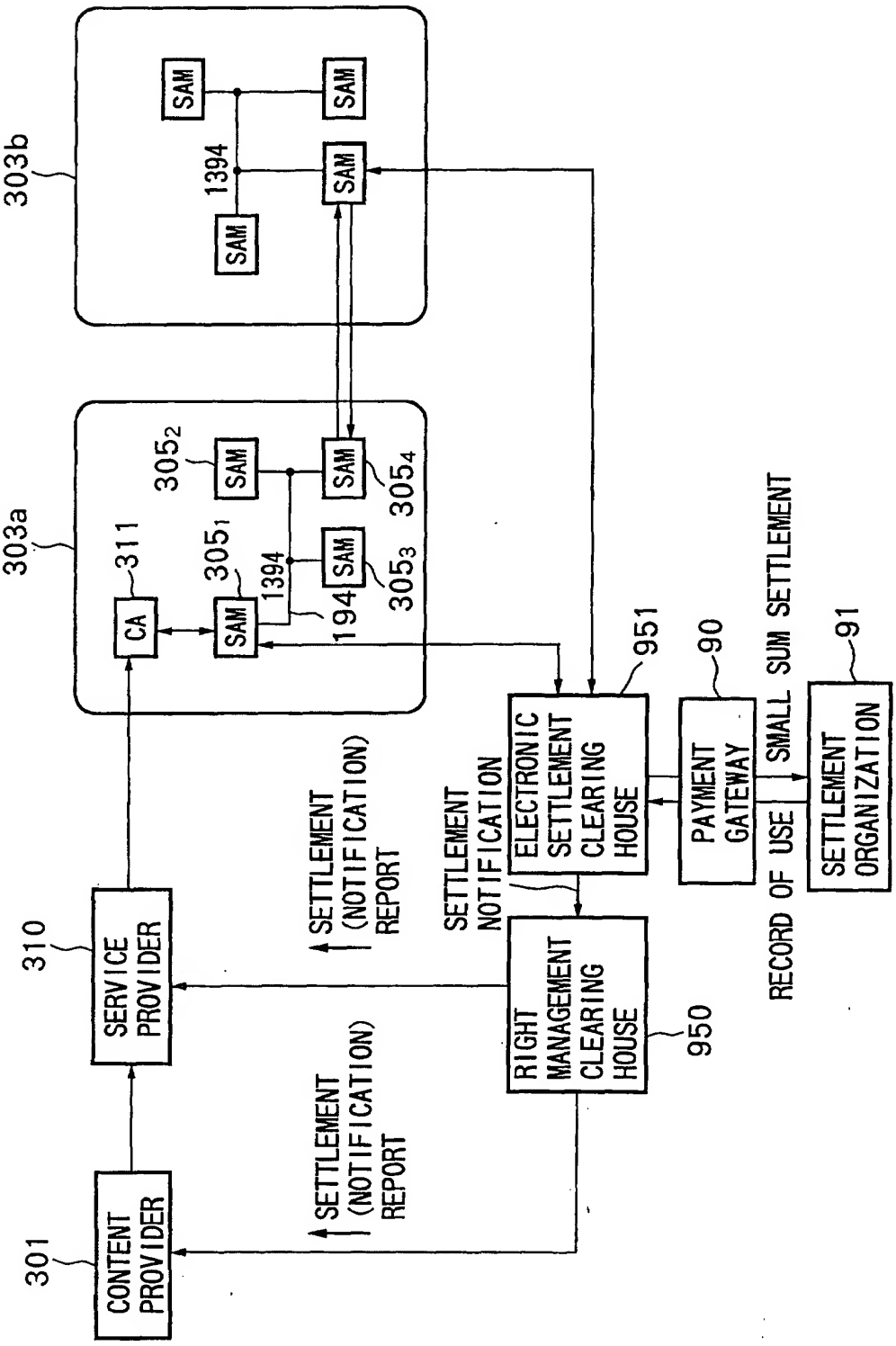

303b
SAM
SAM
1394
SAM
SAM
303a
305_2
SAM
SAM
305_4
311
305_1
1394
SAM
305_3
CA
SAM
194
951
90
91
ELECTRONIC SETTLEMENT CLEARING HOUSE
PAYMENT GATEWAY
SETTLEMENT ORGANIZATION
SMALL SUM SETTLEMENT
RECORD OF USE
SETTLEMENT (NOTIFICATION) REPORT
SETTLEMENT NOTIFICATION
310
SERVICE PROVIDER
RIGHT MANAGEMENT CLEARING HOUSE
950
SETTLEMENT (NOTIFICATION) REPORT
301
CONTENT PROVIDER

FIG.90

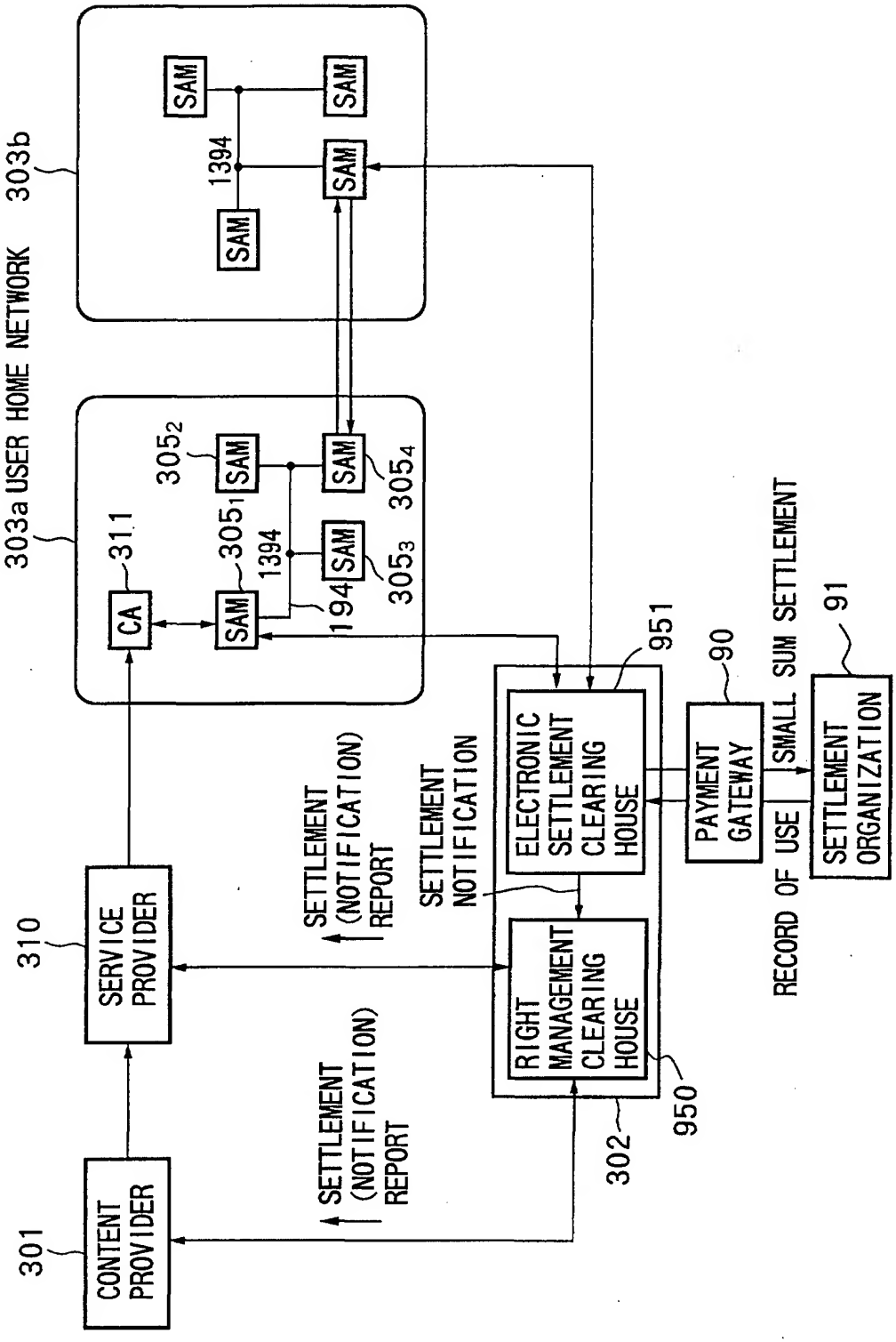

303a USER HOME NETWORK
303b
SAM
1394
CA
311
305_1
305_2
305_3
305_4
194
310
SERVICE PROVIDER
301
CONTENT PROVIDER
SETTLEMENT (NOTIFICATION) REPORT
SETTLEMENT NOTIFICATION
ELECTRONIC SETTLEMENT CLEARING HOUSE
951
RIGHT MANAGEMENT CLEARING HOUSE
950
302
PAYMENT GATEWAY
90
SETTLEMENT ORGANIZATION
91
RECORD OF USE
SMALL SUM SETTLEMENT

FIG.91

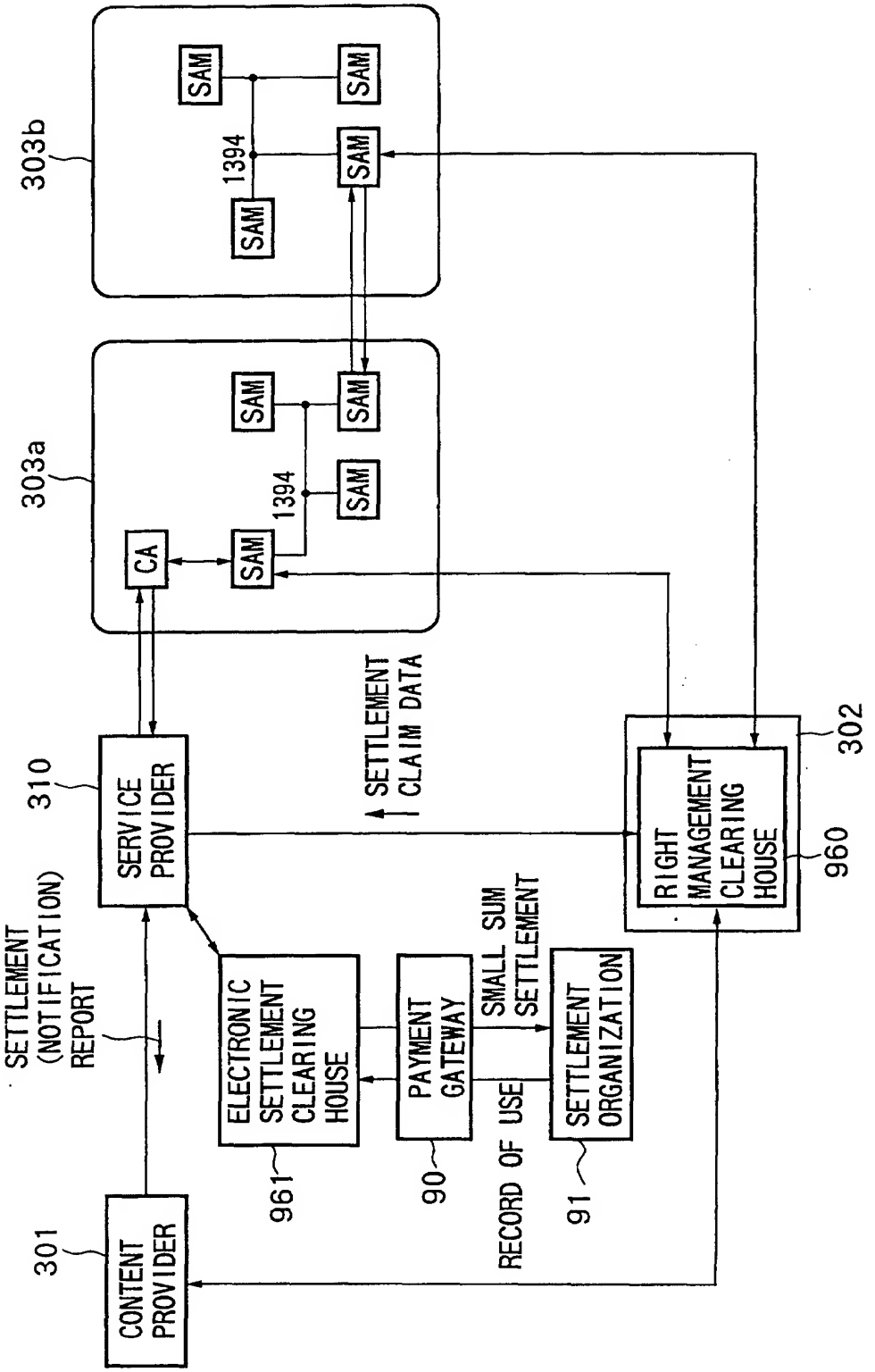

303b
SAM
SAM
1394
SAM
SAM
303a
SAM
SAM
1394
SAM
CA
SAM
SETTLEMENT CLAIM DATA
310
SERVICE PROVIDER
302
RIGHT MANAGEMENT CLEARING HOUSE
960
SETTLEMENT (NOTIFICATION) REPORT
ELECTRONIC SETTLEMENT CLEARING HOUSE
961
PAYMENT GATEWAY
90
SMALL SUM SETTLEMENT
SETTLEMENT ORGANIZATION
91
RECORD OF USE
CONTENT PROVIDER
301

FIG.92

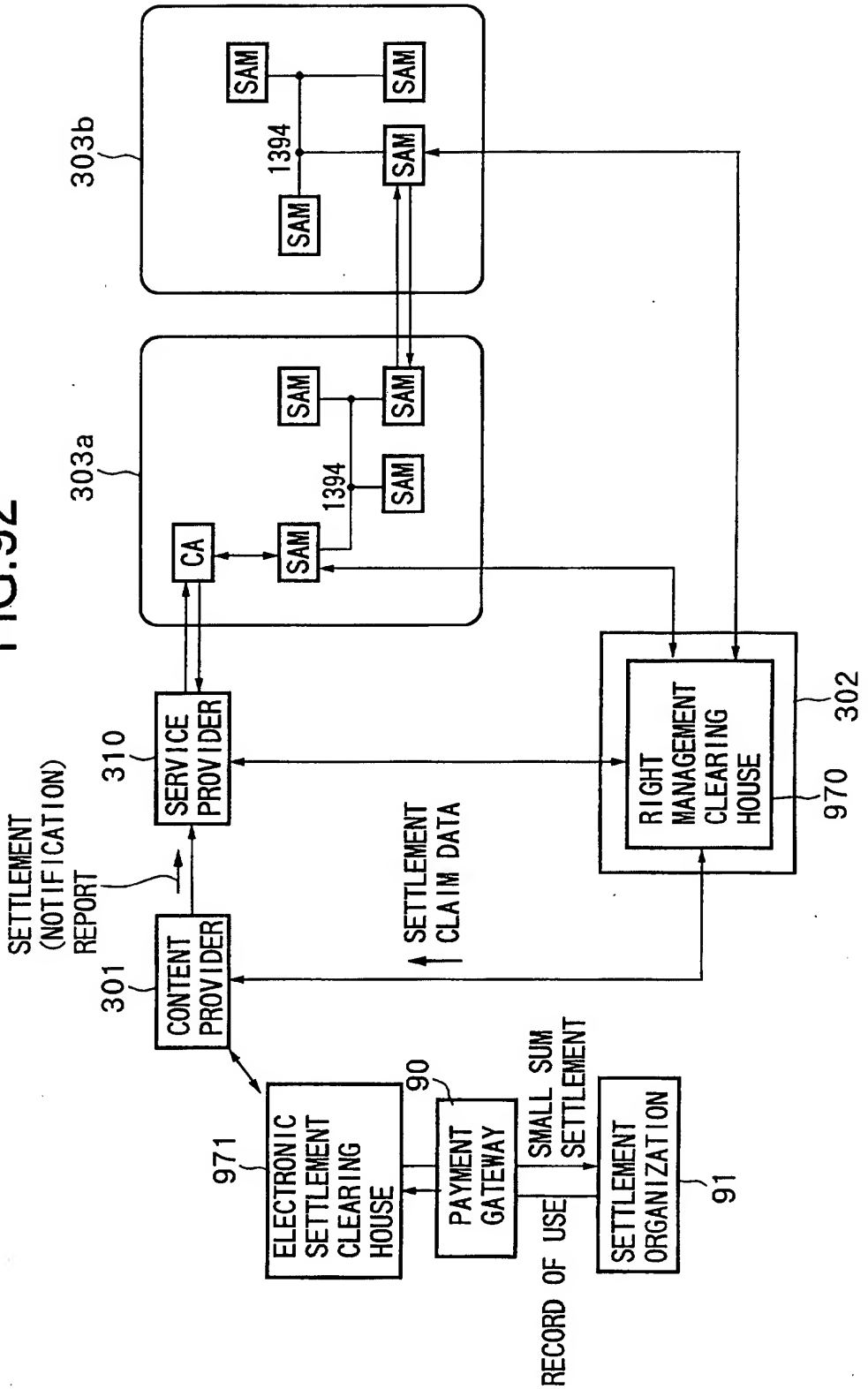
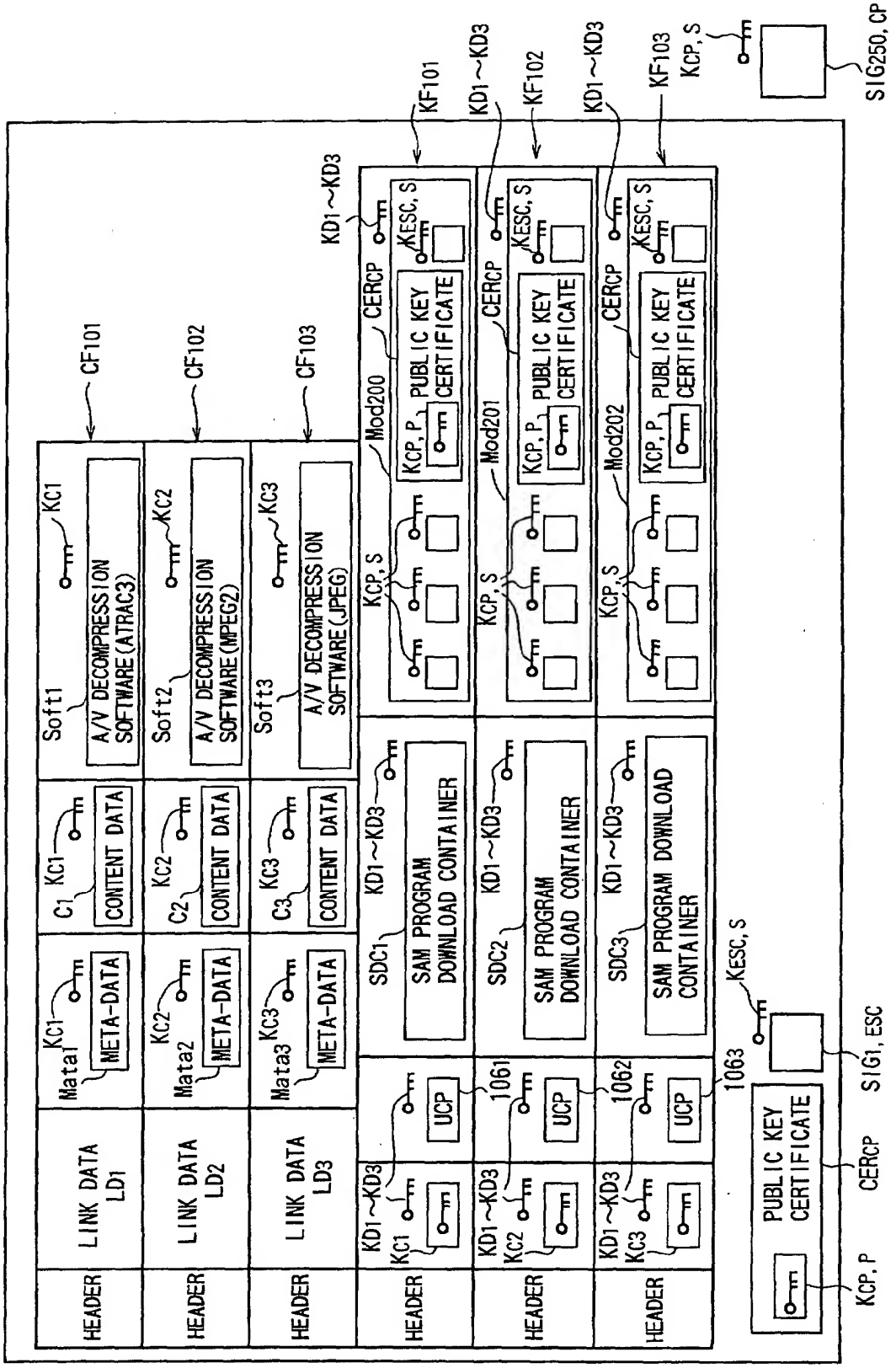

303b
SAM
SAM
1394
SAM
SAM
303a
SAM
SAM
1394
SAM
CA
SAM
SERVICE PROVIDER
310
RIGHT MANAGEMENT CLEARING HOUSE
970
302
SETTLEMENT (NOTIFICATION) REPORT
SETTLEMENT CLAIM DATA
CONTENT PROVIDER
301
ELECTRONIC SETTLEMENT CLEARING HOUSE
971
90
PAYMENT GATEWAY
SMALL SUM SETTLEMENT
RECORD OF USE
SETTLEMENT ORGANIZATION
91

FIG.93

104a SECURE CONTAINER



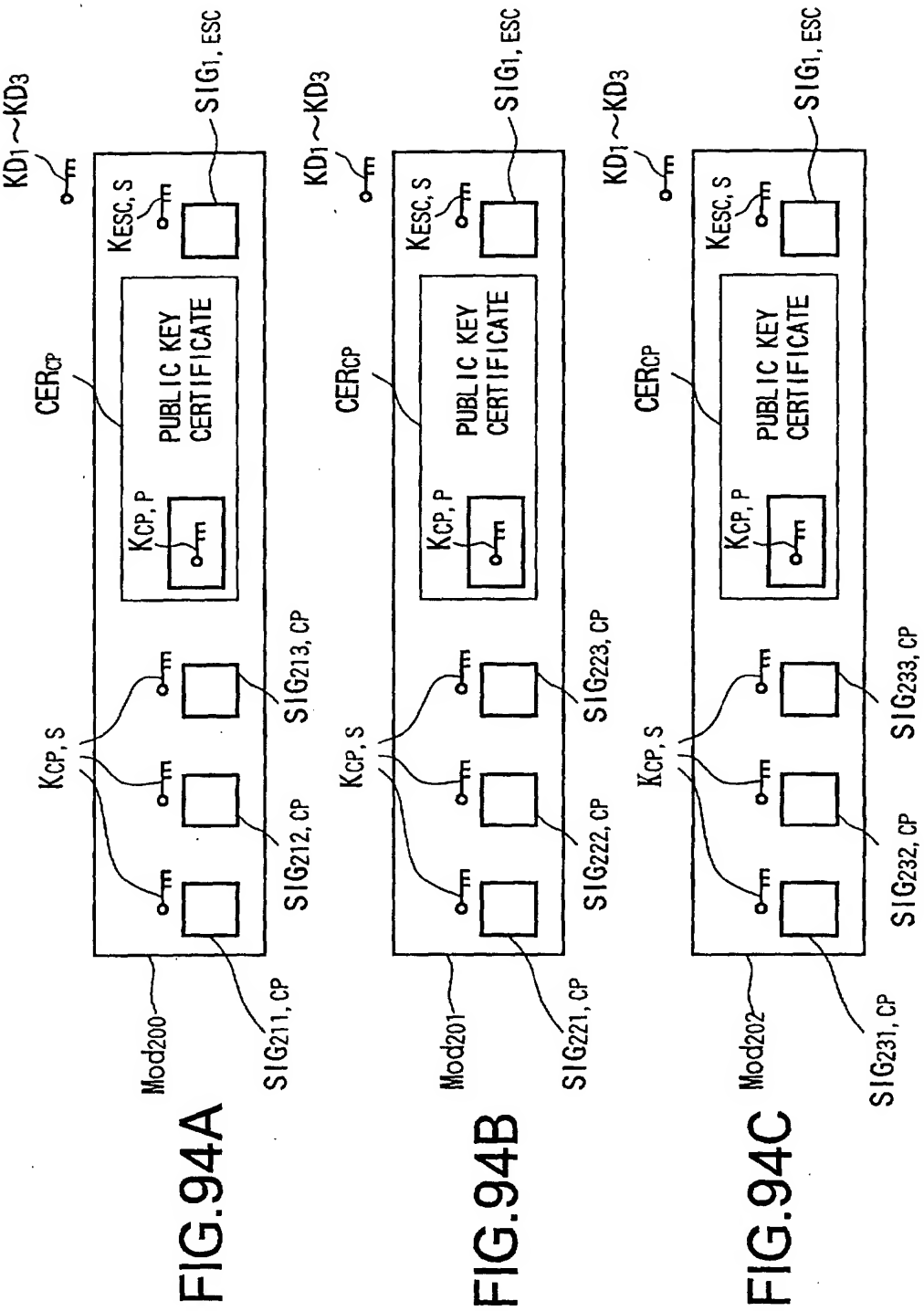


FIG.94A

FIG.94B

FIG.94C

FIG.95

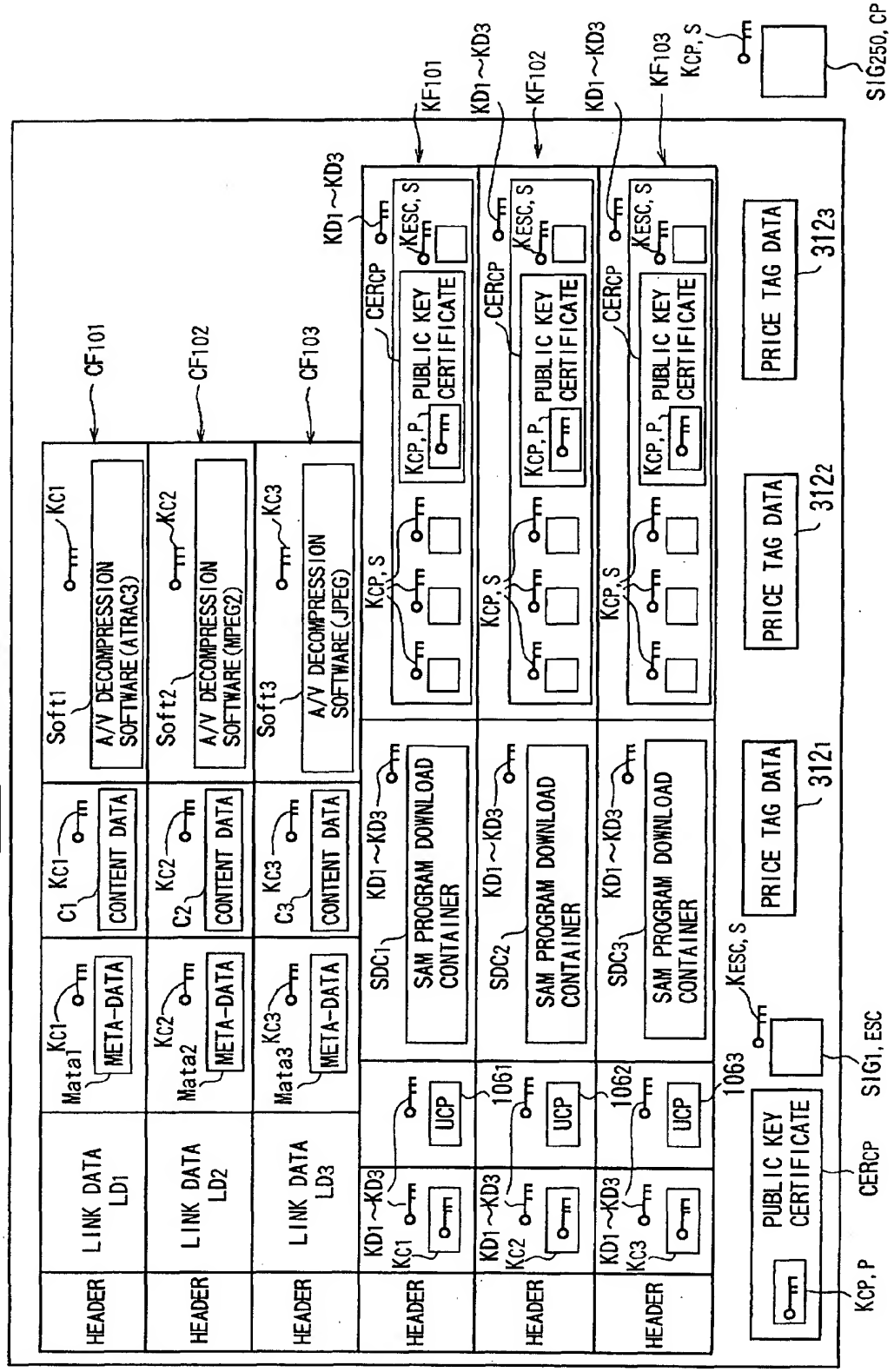

304a SECURE CONTAINER
HEADER
LINK DATA LD1
LINK DATA LD2
LINK DATA LD3
Mata1
Mata2
Mata3
META-DATA
C1
C2
C3
CONTENT DATA
Soft1
Soft2
Soft3
A/V DECOMPRESSION SOFTWARE (ATRAC3)
A/V DECOMPRESSION SOFTWARE (MPEG2)
A/V DECOMPRESSION SOFTWARE (JPEG)
CF101
CF102
CF103
KC1
KC2
KC3
KD1~KD3
KCP, S
KCP, P
PUBLIC KEY CERTIFICATE
CERCP
KESC, S
KF101
KF102
KF103
SDC1
SDC2
SDC3
SAM PROGRAM DOWNLOAD CONTAINER
UCP
1061
1062
1063
PRICE TAG DATA
3121
3122
3123
S1G1, ESC
S1G250, CP

FIG.96

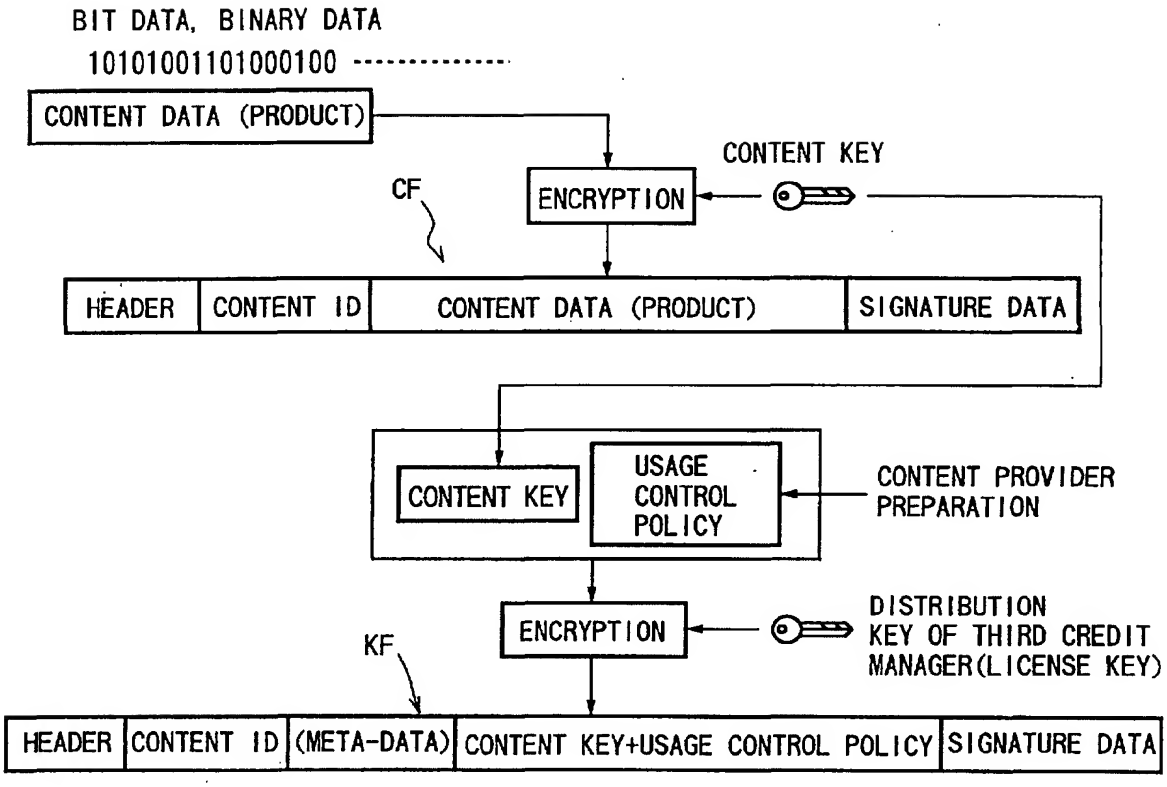

BIT DATA, BINARY DATA
1010100110100100
CONTENT DATA (PRODUCT)
CONTENT KEY
CF
ENCRYPTION
HEADER
CONTENT ID
CONTENT DATA (PRODUCT)
SIGNATURE DATA
CONTENT KEY
USAGE CONTROL POLICY
CONTENT PROVIDER PREPARATION
ENCRYPTION
DISTRIBUTION KEY OF THIRD CREDIT MANAGER(LICENSE KEY)
KF
HEADER
CONTENT ID
(META-DATA)
CONTENT KEY+USAGE CONTROL POLICY
SIGNATURE DATA
INTERNET(FIRST)

FIG.97

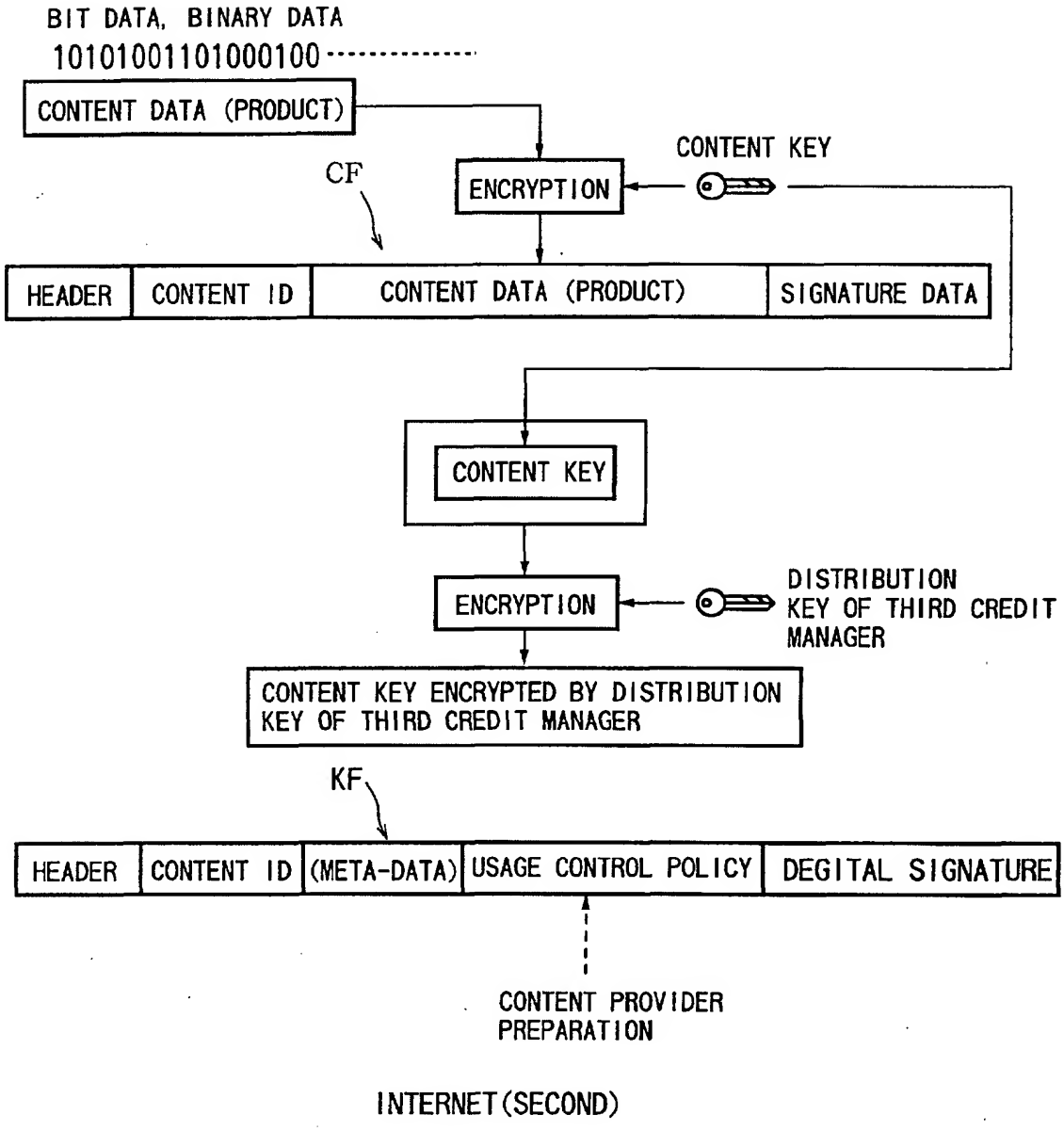
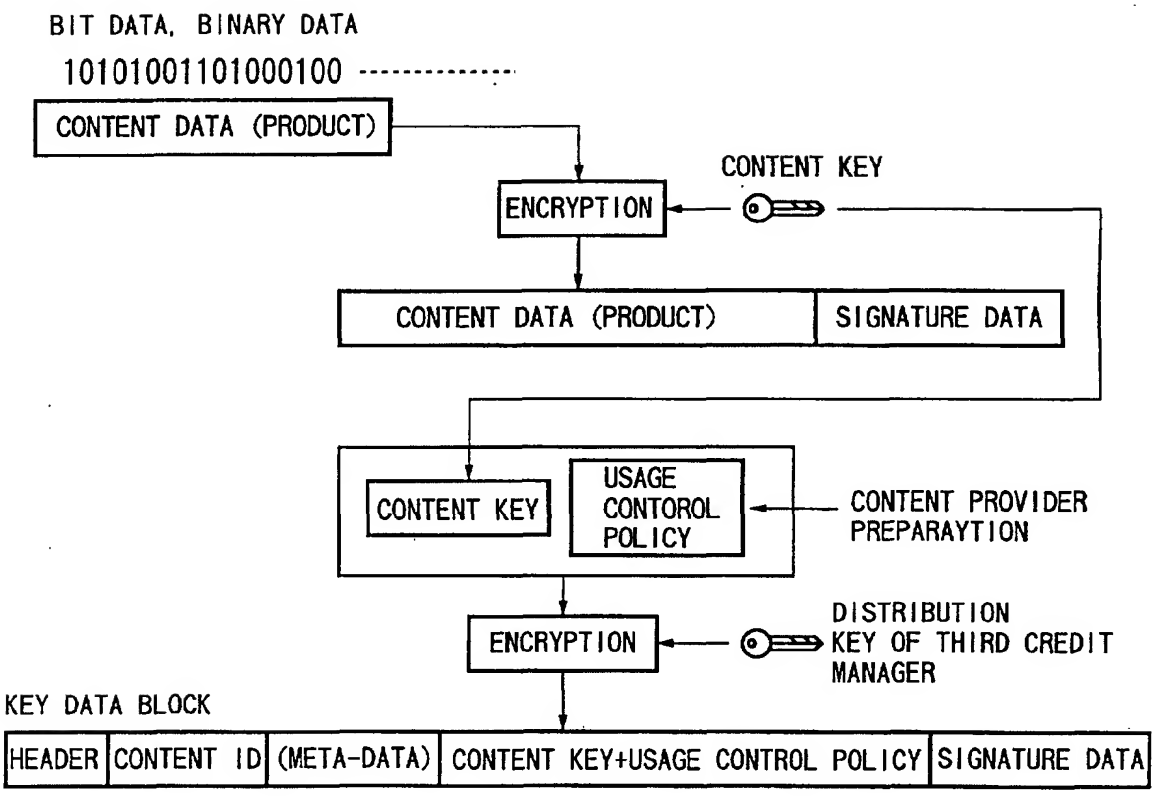

BIT DATA, BINARY DATA
10101001101000100
CONTENT DATA (PRODUCT)
CONTENT KEY
CF
ENCRYPTION
HEADER
CONTENT ID
CONTENT DATA (PRODUCT)
SIGNATURE DATA
CONTENT KEY
ENCRYPTION
DISTRIBUTION KEY OF THIRD CREDIT MANAGER
CONTENT KEY ENCRYPTED BY DISTRIBUTION KEY OF THIRD CREDIT MANAGER
KF
HEADER
CONTENT ID
(META-DATA)
USAGE CONTROL POLICY
DEGITAL SIGNATURE
CONTENT PROVIDER PREPARATION
INTERNET(SECOND)

FIG.98



DIGITAL BROADCAST (FIRST)

FIG.99

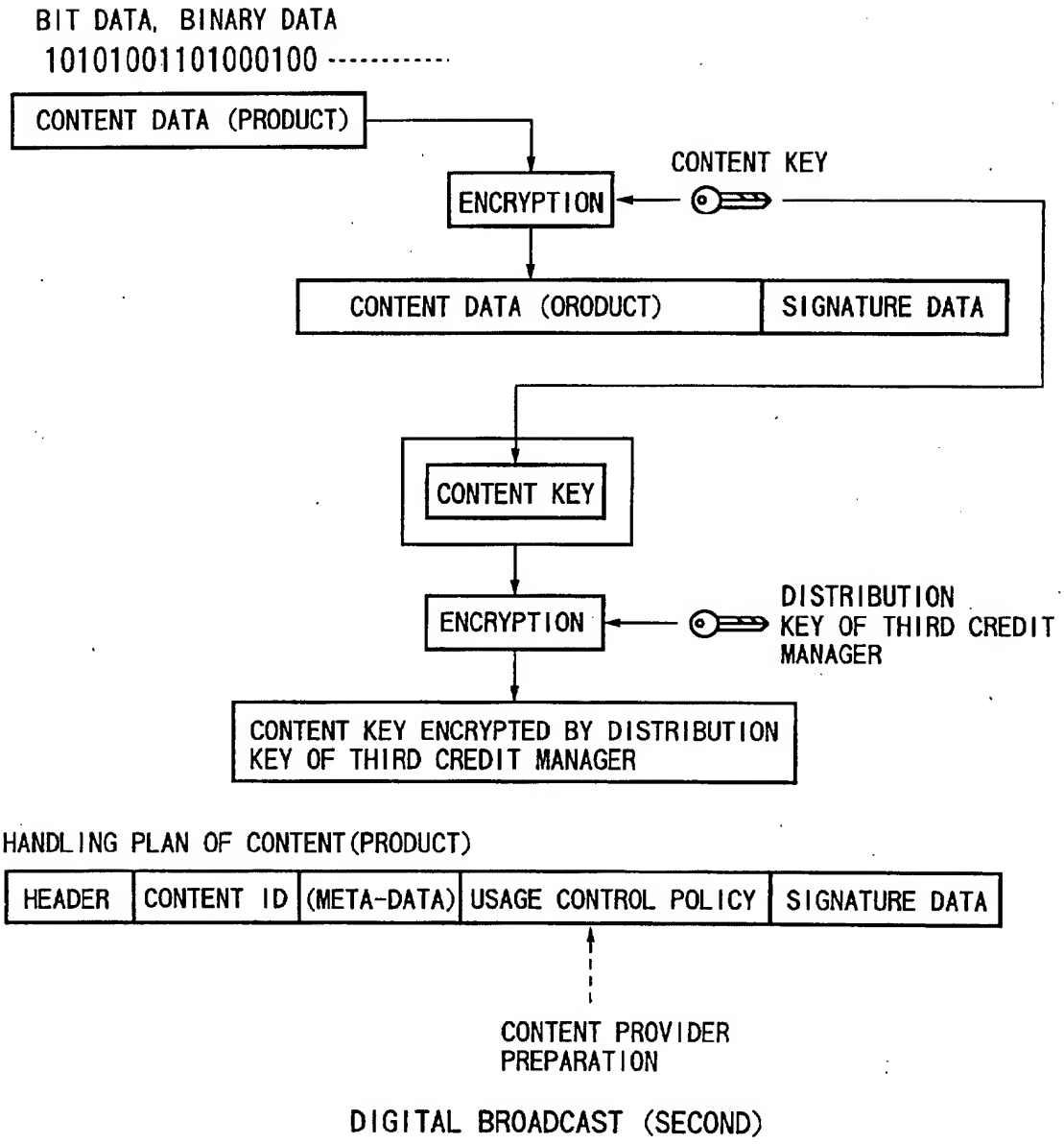
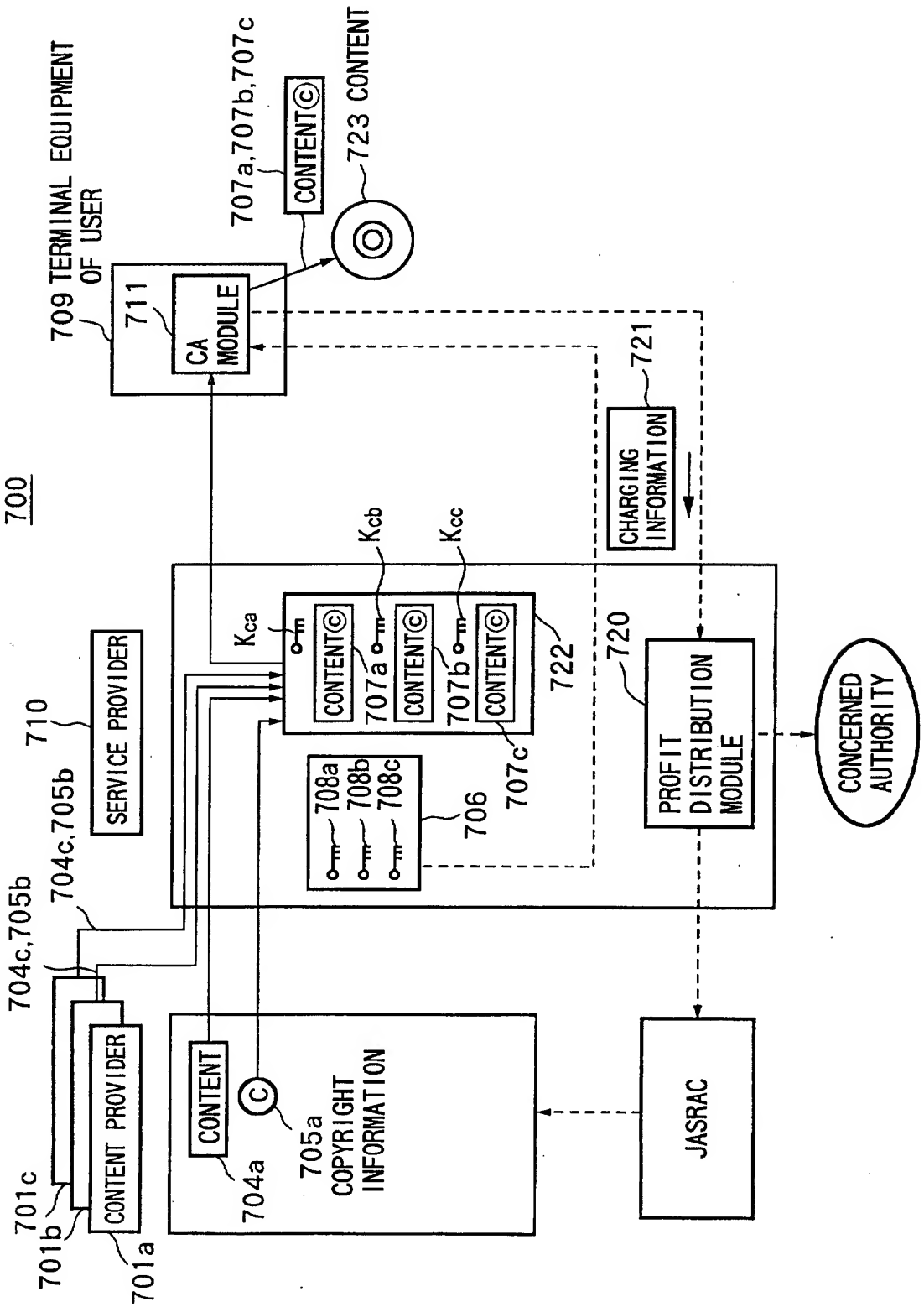

BIT DATA, BINARY DATA
10101001101000100 ----------
CONTENT DATA (PRODUCT)
CONTENT KEY
ENCRYPTION
CONTENT DATA (ORODUCT)
SIGNATURE DATA
CONTENT KEY
ENCRYPTION
DISTRIBUTION KEY OF THIRD CREDIT MANAGER
CONTENT KEY ENCRYPTED BY DISTRIBUTION KEY OF THIRD CREDIT MANAGER
HANDLING PLAN OF CONTENT(PRODUCT)
HEADER
CONTENT ID
(META-DATA)
USAGE CONTROL POLICY
SIGNATURE DATA
CONTENT PROVIDER PREPARATION
DIGITAL BROADCAST (SECOND)

FIG.100


700
709 TERMINAL EQUIPMENT OF USER
711
CA MODULE
707a,707b,707c
CONTENT©
723 CONTENT
721
CHARGING INFORMATION
Kcb
Kcc
Kca
CONTENT©
707a
CONTENT©
707b
CONTENT©
722
720
PROFIT DISTRIBUTION MODULE
CONCERNED AUTHORITY
710
SERVICE PROVIDER
704c,705b
708a
708b
708c
706
707c
704c,705b
CONTENT
704a
©
705a
COPYRIGHT INFORMATION
JASRAC
701c
701b
CONTENT PROVIDER
701a

LIST OF REFERENCES

90... payment gateway

91... settlement organization

92... route certificate authority

100, 300... EMD system

101, 301... content provider

102, 302... EMD service center

103, 304... secure container

105_1 to 105_4, 305_1 to 305_4... SAM

106... usage control policy data

107, 307... settlement report data

108, 308... usage log data

160_1... network apparatus

160_2 to 160_4... AV apparatus

152, 152c, 152s... settlement claim data

191... bus

310... service provider

311... CA module

312... price tag data

CF... content file

KF... key file

Kc... content key data

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP00/04488

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F15/00, G06F17/60, H04L9/08, H04L9/32, G10K15/02, G06F13/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F15/00, G06F17/60, H04L9/08, H04L9/32, G10K15/02, G06F13/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1926-1996 Jitsuyo Shinan Toroku Koho 1996-2000
Kokai Jitsuyo Shinan Koho 1971-2000 Toroku Jitsuyo Shinan Koho 1994-2000

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
CS DATABASE, WPI, JICST SCIENCE and TECHNOLOGY DOCUMENT DATABASE contents, distribution, SuperDistribution

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO, 96/27155, A3 (Electronic Publishing Resources, Inc.), 06 September, 1996 (06.09.96), pages 165 to 177, 386 to 412, 597 to 602, 638 to 644 & JP, 10-512074, W & AU, 9663266, A & EP, 861461, A2 & US, 5910987, A	1-14,16-36, 38-71,142, 150-171, 183-204
Y	& US, 5915019, A & US, 5917912, A & US, 5949876, A & US, 5982891, A	15,37,99-108, 110-115, 117-136, 138-141, 175-182,208
A		72-98,109,116, 137,143-149, 172-174, 205-207
Y	WO, 98/10381, A1 (Intertrust Technologies Corp.), 12 March, 1998 (12.03.98), pages 104 to 142, 168 to 190 (Family: none)	15, 37, 99-108, 110-115, 117-136, 138-141, 175-182,208

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
14 November, 2000 (14.11.00)	21 November, 2000 (21.11.00)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP00/04488

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP, 11-85504, A (Mitsubishi Electric Corporation), 30 March, 1999 (30.03.99), See the full text (Family: none)	1-208
A	JP, 10-161937, A (Toshiba Corporation), 19 June, 1998 (19.06.98), See the full text (Family: none)	1-208

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP00/04488

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

The inventions of the international application are separated into 14 groups: claims 1-71/ claims 72-76, 79-81, 83-89, 92-95, 97/ claims 77, 78, 82, 90, 91, 96, 98/ claims 99-141, 180-182/ claims 142-149/150, 183/ claims 151, 152, 184, 185/ claims 153, 154, 186, 187/ claims 155-157, 160-165, 188-190, 193-198/ claims 158, 191/ claims 159, 192/ claims 166-171, 199-204/ claims 172-174, 205-207/ and claims 175-179, 208.

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest
☐ The additional search fees were accompanied by the applicant's protest.
☐ No protest accompanied the payment of additional search fees.

Form PCT/ISA/210 (continuation of first sheet (1)) (July 1992)